Recht en web 2.0

Lodder, A.R.; van den Hoven van Genderen, R.; Engelfriet, A.; Mekic, D.; Wisman, Tijmen

2010

Recht en Web 2.0

Arno R. Lodder
Rob van den Hoven van Genderen
Arnoud Engelfriet
Danny Mekic´
e.a.

Studiecommissie Recht en Web 2.0

No. 27 Publicatiereeks NVvIR

NVvIR - Nederlandse Vereniging voor
Informatietechnologie en Recht,
2010

Recht en Web 2.0

Bewerkte bloemlezing uit www.internetrecht20.nl

Arno R. Lodder
Rob van den Hoven van Genderen
Arnoud Engelfriet
Danny Mekic´
Amanda van Rij
Erik Vogelzang
Ineke Schouwstra
July Rattan
Kwame Agyapong-Ntra
Leonoor van Wijnbergen
Maaike Verwoest
Manon Wesseling-Vlaanderen
Sebastiaan Brommersma
Teun Burgers
Tijmen Wisman
Trevor Waal
Tugrul Sakaoglu

Studiecommissie Recht en Web 2.0

No. 27 Publicatiereeks NVvIR

NVvIR - Nederlandse Vereniging voor Informatietechnologie en Recht,
2010

Voorwoord

Op 17 juni 2008 vond een bijeenkomst plaats met de leden van de studiecommissie Recht en Web 2.0. Aan het eind van de bijeenkomst was het Nederlands elftal inmiddels begonnen aan de derde groepswedstrijd van het Europees kampioenschap tegen Roemenie. De vraag was of we die beelden later nog op Youtube terug zouden kunnen zien. Van een eerdere wedstrijd tijdens dat toernooi waren de beelden van een sfeerimpressie uit een cafe door de maker daarvan namelijk op Youtube geplaatst. Youtube is een van de populairste Web 2.0 toepassingen. De beelden bleven niet lang staan, omdat door het laten zien van de doelpunten en andere acties uit de wedstrijd de auteursrechten van de UEFA zouden zijn geschonden. Dit was althans naar de mening van deze voetbalorganisatie het geval.

De juridische relevantie van veel van de beelden die worden geupload is auteursrechtelijk van aard, met privacy als een goede tweede. Meer in het algemeen zijn het vooral inbreuken op de persoonlijke levenssfeer en het auteursrecht die spelen bij Web 2.0 toepassingen. Hierin onderscheidt dit onderwerp zich niet van het internetrecht in het algemeen, waar deze onderwerpen een prominent onderdeel van zijn. In dit boek zal duidelijk worden dat de achtergrond en omvang van Web 2.0 een afzonderlijke bestudering rechtvaardigt.

Tijdens de najaarsvergadering van de NVvIR over Recht en Web 2.0 op 20 november 2008 waren twee lezingen aan de centrale juridische onderwerpen gewijd. Martin Senftleben besprak de relevantie van Intellectuele Eigendom en Sjoera Nas behandelde de juridische aspecten van privacy. Daarnaast gingen de lezingen over de bijdragen van de user community aan het product TomTom door Simon Hania en over netneutraliteit door Machiel Bolhuis van Google.

In dit boek zullen deze en andere juridische invalshoeken van Web 2.0 belicht worden. Uiteraard zal eerst worden ingegaan op wat nu precies onder Web 2.0 moet worden verstaan.

Het voorliggende boek is anders opgebouwd dan u gewend bent. Doorgaans wordt in rond de 5 hoofdstukken een onderwerp door

verschillende auteurs behandeld. Dit boek is in het geheel door een vrij grote groep auteurs geschreven. Of beter, de auteurs hebben hun bijdragen ge-upload naar de wiki Internetrecht 2.0 (www.internetrecht20.nl), die ook na de totstandkoming van dit boek in de lucht zal blijven. De bijdragen zijn op alle onderwerpen geleverd zonder specifieke hoofdstukverdeling. Een ieder wordt uitgenodigd om ook na verschijnen van dit boek aanvullingen of verbeteringen in de wiki aan te brengen.

Van de oorspronkelijke studiecommissie waren uiteindelijk maar enkelen bestand tegen de vrijheid/vrijblijvendheid die het uploaden van content naar de wiki inhoudt. Het gros van de auteurs bestaat uit studenten die het vak Actualiteiten Internetrecht aan de Vrije Universiteit in het najaar van 2008 volgden. Het voorliggende boek is een gedeeltelijk bewerkte en op veel punten aangevulde en nader uitgewerkte bloemlezing van al die bijdragen. De tekst is juni 2010 afgesloten (en gedrukt), waardoor verschillende ontwikkelingen sinds najaar 2008 konden worden meegenomen.

Om de cirkel rond te maken, tijdens het Wereldkampioenschap voetbal in Zuid-Afrika is dit boek afgerond. Behalve vanwege de gebruikelijke redenen, heeft het zo lang geduurd omdat verschillende bijdragen van de Wiki niet van voldoende kwaliteit waren. Een wiki ontleent zijn kracht aan de correctie van de massa, maar bij de wiki internetrecht20.nl bestonden de bijdragen te vaak uit door een enkele deelnemer geplaatste informatie die vervolgens onvoldoende verbeterd werd door anderen. Hiermee is niet gezegd dat er geen bijzonder goede en voldragen stukken op de wiki te vinden zijn. Er zaten echter ook bijdragen tussen die, al dan niet onder verwijzing naar de bron, letterlijk van een internetpagina waren overgenomen. Een andere reden voor de vertraging was dat een verzameling wiki-stukken nog geen coherent boek maakt. Dit laatste hebben we, aangevuld met een groot aantal teksten die niet op de wiki te vinden zijn, in de achterliggende periode trachten te realiseren. Hoewel de ontwikkelingen zoals met ieder internetrecht onderwerp niet stil staan, verwachten we met dit boek een adequaat overzicht te geven.

Arno R. Lodder & Rob van den Hoven van Genderen
Amsterdam, 2008-2010

Inhoudsopgave

1 Inleiding

De afgelopen jaren is het aanbieden van content op internet steeds meer in handen gekomen van de oorspronkelijke afnemers. Web 2.0 is de verzamelnaam voor een nieuwe manier van omgaan met het World-Wide Web. Websites zijn geen geïsoleerde silo's meer waarin een kleine, professionele redactie publiceert en de bezoeker braaf consumeert wat hem wordt aangeboden Web 2.0 stelt sociale interactie tussen natuurlijke personen centraal.

De gebruikers, of liever gezegd de deelnemers, leveren zelf de inhoud, in de vorm van discussies, reacties, informatie over zichzelf, enzovoorts. Men bouwt een Hyves-profiel, publiceert het CV in LinkedIn of Monsterboard en discussieert mee op forums, wiki's en andere sociale netwerksites (zoals Facebook en MySpace). Volgens een onderzoek uit 2008 van Marktonderzoeksbureau Synovate[1] zou zelfs 89% van de Nederlanders weten wat een sociale netwerksite is en heeft Nederland relatief gezien de meeste leden van dergelijke sociale netwerksites. Meer dan de helft van de Nederlanders is op een of meerdere sociale netwerksites te vinden. Deze percentages zeggen nog niet iets over de wijze van deelnemen, want er zijn een behoorlijk aantal deelnemers die op uitnodiging van een al dan niet virtuele vriend zich aansluiten bij een sociale netwerksite en er vervolgens niets mee doen. Dit is een onderdeel van de strategie van de aanbieders, veelal is het zelfs niet mogelijk de pagina´s van deelnemers te bekijken zonder zelf lid te worden. Dit toelatingsbeleid versterkt het communitykarakter van dergelijke sites, maar werkt ook in de hand dat deelnemers zich enkel registreren met het doel eenmalig of bij gelegenheid profielen te bekijken zonder zelf content aan te dragen.

1.1 Web 2.0, 3.0 en The Internet of Things

Toen begin jaren negentig het internet voor het algemeen publiek werd opengesteld, konden met de op zich revolutionaire Mosaic browser nog weinig informatiebronnen worden geraadpleegd. Door

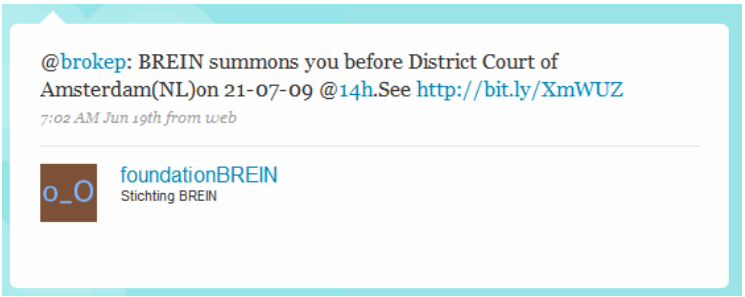
[1] http://www.synovate.nl/nieuws/20081009001/news.aspx

deze nieuwe toepassing werd het mogelijk documenten van verschillend formaat via dezelfde interface te openen. Ook werden nu in een en dezelfde toepassing verschillende protocollen als ftp en uiteraard http ondersteund.[2]

In deze beginperiode werd de informatie op internet door in meerderheid grote aanbieders, zoals universiteiten en de indertijd al populaire internet movie database,[3] ter beschikking gesteld. Vanaf 1995 vond een eerste omslag plaats doordat zich steeds meer commerciële aanbieders als Amazon, CDnow, etc. op de markt gingen bewegen. Het aanbieden van informatie door vooral grote aanbieders wordt als de oervorm van het World Wide Web gezien en aangeduid met de term Web 1.0.[4] Het voor de regulering van de elektronische handel centrale concept *dienstverlener van de informatiemaatschappij* (artikel 3:15d lid 3 BW) moet ook in het licht van dergelijke aanbieders worden gezien.

Een belangrijke ontwikkeling waarbij de gebruikers de macht in handen kregen waren de P2P netwerken zoals Napster, KaZaa[5] en de in 2009 in Zweden veroordeelde aanbieders van The Pirate Bay.[6] Deze laatste aanbieder geniet ook bekendheid door het proces dat BREIN in Nederland tegen de eigenaren van de site heeft aangespannen.[7] Behalve dat de aanbieder The Pirate Bay een Web 2.0 dienst levert, is het proces vooral ook bekend omdat bij de dagvaarding gebruik gemaakt werd van Web 2.0 toepassingen. Zo werd een verwijzing naar de dagvaarding op Twitter achtergelaten.

[2] Voor de volledigheid: respectievelijk File Transfer Protocol en Hyper Text Transfer Protocol.
[3] http://www.imdb.com
[4] Deze term Web 1.0 werd uiteraard pas gebruikt op het moment dat Web 2.0 als term werd geïntroduceerd.
[5] Hoge Raad 19 december 2003, LJN AN7253 (KaZaa), met noot Hugenholtz, *AMI 2004/1,* p. 9-25 ook verschenen in T. van der Linden-Smith & A.R. Lodder (red.)(2006), *Jurisprudentie Internetrecht Annotaties*, Kluwer, Deventer.
[6] Zie over deze Zweedse zaak B.W. Schermer (2009), De Pirate Bay uitspraak: aansprakelijkheid van internetdienstverleners opgehelderd? *Tijdschrift voor Internetrecht* (3), pp. 68-71.
[7] Onder andere Vzr. Amsterdam 30 juli 2009 (LJN BJ4298), Vzr. Amsterdam 30 juli 2009 (LJN BJ4466) en Vzr. Amsterdam 22 oktober 2009 (BK1067).



De advocaten werden ook voor korte tijd virtuele vrienden met de eigenaren van The Pirate Bay en konden zo via Facebook de dagvaarding achterlaten. Dat deze dagvaarding goed aangekomen was, bleek toen ze binnen een minuut na achterlating van de dagvaarding weer "ontvriend" werden. In de (inter)nationale pers is uitgebreid aandacht aan deze wijze van dagvaarden besteed.[8]

Bij aanbieders van P2P-netwerken (ook wel bestandsuitwisselingsdiensten genoemd) zoals Napster, KaZaa en The Pirate Bay stelt de gebruiker content aan andere gebruikers ter beschikking. Een op conceptueel niveau vergelijkbaar model[9] wordt gebruikt bij veilingsites als Marktplaats en eBay, waar ook de aanbieder (als neutrale derde) partijen die elkaar in beginsel niet (hoeven te) kennen bij elkaar probeert te brengen. Een op content niveau vergelijkbare dienst vormen is het downloaden van iTunes bestanden, waarbij de content overigens wel door een grote aanbieder in klassieke Web 1.0 zin wordt geleverd, namelijk Apple.

Interactie is een belangrijk kenmerk van Web 2.0. Dit kan het ter beschikking stellen en delen van feitelijke informatie middels Wiki's zijn, maar ook het ter beschikking stellen en delen van persoonlijk informatie (denk hierbij bijvoorbeeld aan sociale netwerksites als Hyves). Doordat de interactie op het internet plaatsvindt, wordt iedere gebruiker in staat gesteld een uitgever (blog) of omroep te worden (Youtube). Het oude internet ideaal van de artiest

[8] Zie onder andere *Pirate Bay Founders Served Court Summons Via Twitter* (exclaim.ca), *The Pirate Bay Receives Court Summons Via FaceBook and Twitter* (http://www.zeropaid.com/), *Pirate Bay served with Dutch lawsuit via Twitter and Facebook* (http://www.thelocal.se/20244/20090624/) en Nederlandse blogs hierover http://blog.iusmentis.com/2009/06/25/gedagvaard-via-twitter-kan-dat/ alsmede http://jurel.nl/2009/06/26/douwe-groenevelt-probeert-the-pirate-bay-de-rechtszaal-in-te-twitteren/

[9] Op technisch niveau zijn de diensten niet te vergelijken.

die zonder platenmaatschappij een publiek kan bereiken is hiermee gerealiseerd, zij het dat eenmaal doorgebroken (bijv. de Nederlandse Esmee Denters via Youtube) de platenmaatschappijen een artiest weer kunnen inlijven.

Een volgende stap in de evolutie van het internet is Web 3.0, waarbij niet langer informatie wordt doorgeven zonder dat de gebruikte toepassingen begrijpen waar het over gaat, maar met kennis van zaken. Deze kennis is als meta-informatie aan internetpagina's toegevoegd. Als een (internet)jurist zoekt naar Martijn zal deze als eerste de uitspraak uit 2007 inzake provideraansprakelijkheid krijgen[10] of de suggestie "Zoekt u...?". De aan internetpagina's toegevoegde informatie in combinatie met gebruikersprofielen zal tot een verbeterde informatievoorziening moeten leiden. Web 3.0 staat ook wel bekend als het Semantic Web.[11]

De voorgangster van Neelie Smit-Kroes, de Europees commissaris voor de informatietechnologie Viviane Reding, heeft in 2008 aangegeven voor Europa een belangrijke rol te zien bij de ontwikkeling en totstandkoming van Web 3.0:[12]

> "Web 3.0 betekent naadloos netwerken voor zaken, vrije tijd en op sociaal vlak overal en altijd met behulp van snelle, betrouwbare en veilige netwerken. Het betekent het eind van de kloof tussen mobiele en vaste lijnen."

De Europese Commissie is de mening toegedaan dat Web 3.0 inhoudt dat niet alleen consumenten maar ook bedrijven vaker online diensten gebruiken, televisie mobiel bekeken wordt en dat men meer tijd op sociale netwerken doorbrengt. De EU gelooft dat Europa het voortouw kan nemen in de gang naar Web 3.0 maar ziet ook een schaduwzijde: de Commissie vreest dat Web 3.0 een bedreiging voor de privacy kan betekenen. Dit gevaar is te meer reëel omdat Web 3.0 in verband gebracht wordt met het zogenaamde 'internet van dingen'.[13] Denk hierbij aan de slimme ener-

[10] Vzr. Amsterdam 1 november 2007 (LJN: BB6926), zie ook http://jurel.nl/2007/11/01/koninklijke-foto's-terechte-specific-obligation-to-monitor/

[11] Tim Berners Lee (1998), *Semantic Web Road map* http://www.w3.org/DesignIssues/Semantic.html en het handboek G. Antoniou & F. van Harmelen (2008), *A Semantic Web Primer* (2nd Edition), MIT Press.

[12] Zie ook *The Future Internet: Service Web 3.0* (http://www.youtube.com/watch?v=off08As3siM) alsmede een filmpje van het Elektronisch Platform Nederland (inmiddels gefuseerd met ECP) *Evolution Web 1.0, Web 2.0 to Web 3.0* (http://www.youtube.com/watch?v=bsNcjya56v8)

[13] Tijmen Wisman doet sinds mei 2010 naar dit onderwerp promotie-onderzoek aan de VU, bij het Computer/Law Institute (afdeling Transnational Legal Studies).

giemeter,[14] automatische kentekenherkenning, de OV chip card, het koppelen van camera-observatie aan databases met gezichtskenmerken en de klassieke voorbeelden: de intelligente koelkast (die ziet wanneer de melk op is) en de intelligente wasmachine (die vaststelt dat een rode broek niet bij witte lakens moet). Het internet van dingen staat niet op zichzelf, maar hangt samen met de opkomst van een nieuw paradigma, waarin ook termen als 'ubiquitous computing',[15] en 'ambient intelligence'[16] thuishoren.

Of Europa ook daadwerkelijk een voorname rol zal kunnen spelen is niet zeker, aangezien men op Europees niveau nog niet goed raad weet met de privacyaspecten van Web 2.0. Dit betreffen echter juridische aspecten, op technisch terrein speelt Europa zeker een belangrijke rol, onder andere via een groot aantal door de EU gesteunde projecten. De plannen zijn er in ieder geval, de verwachtingen van de Europese Unie zijn hooggespannen:[17]

> "Foreshadowing 'the Future Internet', the implementation of the Internet of Things will help to meet a considerable number of current challenges such as an ageing society, deforestation or CO2 emissions through the development in particular of health monitoring systems, connected trees and cars. The interconnection of physical objects will generate a genuine paradigm shift for society."

Binnen dit internet van de toekomst verwacht de EU een voortrekkersrol te kunnen vervullen:

> "(…) IoT [Internet of Things, ARL/RvdHvG] is not yet a tangible reality, but rather a prospective vision of a number of technologies that, combined together, "could in the coming 5 to 15 years drastically modify the way our societies function. By adopting a proactive approach, Europe could play a leading role in shaping how IoT works and reap the associ-

[14] www.slimmeenergiemeter.nl
[15] Hieronder wordt verstaan: "developing systems and technologies that automatically locate people, equipment, and other tangibles", zie J. Hightower & G. Borriello (2001), "Location Systems for Ubiquitous Computing ," *COMPUTER*, Vol. 34, 08, pp. 57-66, AUGUST, 2001.
[16] Hiermee wordt bedoeld: „electronic environments that are sensitive and responsive to the presence of people", zie B. de Ruyter & E. Aarts (2004) Ambient intelligence: visualizing the future. In *Proceedings of the Working Conference on Advanced Visual interfaces* (Gallipoli, Italy, May 25 - 28, 2004). AVI '04. ACM, New York.
[17] Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things: an action plan for Europe COM(2009) 0278 final.

> ated benefits in terms of economic growth and individual well-being, thus making the Internet of things an Internet of things for people."

Nog verder in de toekomst zou Web 4.0 liggen, waarvan enkel vage contouren te ontwaren zijn:[18]

> "(…)Web 4.0 (…) is really hazy (…) implies that machine intelligence has reached a point that the Internet becomes the planetary computer, a massive web of highly intelligent interactions."

Het is de vraag hoe zinvol dit doornummeren vanaf 2.0 is en zeker verder dan 3.0. Vrijwel niemand is in staat een goede, sluitende definitie van Web 2.0 te geven en in de omschrijvingen van Web 3.0 en eventuele opvolgers is veel overlap te vinden. Het is goed om te beseffen dat het internet voortdurend doorontwikkelt, de precieze termen daarvoor zijn minder van belang.[19] In ieder geval beperken we ons tot Web 2.0 en verwachten dat zeker na lezing van dit boek duidelijk is wat hieronder begrepen moet worden.

1.2 Recht en Web 2.0

In dit boek staat de juridische analyse van Web 2.0 toepassingen centraal. Hoe dienen aanbieders van Web 2.0 diensten om te gaan met de gegevens die wij hen leveren? En wat is de rol van deze aanbieders indien de gegevens een strafbare inhoud hebben, zoals bij de verspreiding van racistische uitingen of kinderporno via openbare en min of meer privé chatsites, denk bijvoorbeeld aan Windows Live Messenger (voorheen MSN-Messenger) of de vele internetdiscussiefora. Nu de toepassing van het internet verandert kan men zich afvragen of de verantwoordelijkheden van overheden over wat zich op het internet afspeelt niet moet mee veranderen. Hoe dienen overheden om te gaan met virtuele werelden? Hoe dient de overheid om te gaan met steeds actievere internet-

[18] Dan Farber, *From semantic Web (3.0) to the WebOS (4.0)*, http://www.zdnet.com/blog/btl/from-semantic-web-30-to-the-webos-40/4499

[19] Zie ook Jon Mell, *Web 2.0, Web 3.0, Web 4.0, Web 5.0 – where will it end?*, http://jonmell.co.uk/web-20-web-30-web-40-web-50-where-will/: „Already people are starting to talk about Web 3.0 just to be the first clever person to come up with it because it's so easy just to add 1 to Web 2.0 and get Web 3.0. Usually, the way things work is that you notice a trend, and then coin a phrase. With Web 3.0+ it's backwards – we already know what the next development in web technology will be called, we just don't know what it is yet."

gebruikers die veel gegevens over zichzelf maar ook anderen op internet plaatsen? In hoofdstuk 9 wordt afzonderlijk ingegaan op het lastige vraagstuk hoe eenmaal op internet verschenen persoonlijke informatie kan worden verwijderd.

Ook het auteursrecht wordt in nog verdergaande mate dan bij internet in het algemeen het geval is op de proef gesteld. De al eerder genoemde P2P-netwerken illustreren in versterkte mate het nauwelijks meer vol te houden onderscheid tussen illegaal uploaden en legaal downloaden. Op zich is deze insteek in Nederland ook op ander vlak bekend, namelijk bij de handel in soft drugs. Hier geldt kortweg dat de softdrugs er uit mogen door de voordeur (verkoop), maar er niet in mogen bij de achterdeur (inkoop). Bij softdrugs geldt een kwantitatief criterium, tot een bepaalde hoeveelheid wordt het bezit ervan toegestaan of beter, omdat het wettelijk verboden is, gedoogd. Bij muziekbestanden is het uploaden van een enkel bestand al in strijd met het auteursrecht, terwijl er in beginsel een eindeloze reeks aan muziekbestanden legaal gedownload mogen worden.

Het aantal inbreuken op auteursrecht dat dagelijks op internet plaatsvindt, is niet te tellen. Steeds vaker maken gewone consumenten inbreuk op auteursrechten van anderen en lang niet altijd realiseren ze zich dit. Illustratief is een moderne tekstvariant van het nummer Radio Gaga van Queen dat oorspronkelijk handelde over de opkomst van de radio:

> "And everything we want to get,
> We download from the internet,
> No need to think, no need to feel,
> When only cyberspace is real"[20]

Soms betreft het onschuldige inbreuken waarbij het sanctioneren niet direct op sympathie kan rekenen, zoals het aan een jeugdige internetgebruiker verzenden van een notice-and-takedown brief op grond van de Amerikaanse Digital Millenium Copyright Act (DMCA) omdat er op een site plaatjes van My Little Pony te vinden zijn.[21] Of de puber die een website over voetbal beheert en meer dan vierduizend euro moet betalen aan de fotograaf van een foto

[20] Uit de Musical *We Will Rock You* van Queen en Ben Elton, enkele jaren terug vertoond in London, in de zomer van 2010 aangekondigd voor Nederland.
[21] De producent (Hasbro) van deze speelpony's met gekleurde huid en haren heeft hier zich in ieder geval in het verleden aan schuldig gemaakt.

van Johan Cruyff die nota bene niet door hemzelf op de site is geplaatst.[22]

Zoals eerder aangegeven wordt de rol van traditionele producenten van informatie (zoals uitgevers) in toenemende mate overgenomen door de internetgebruikers zelf. Er worden films en foto's geüpload, blogs geschreven, hele doopcelen al dan niet op eigen initiatief gelicht en dit alles doorgaans inclusief commentaar van andere gebruikers (goodies, discussie, feedback, etc.). De verschillende diensten kunnen in veel gevallen worden gecombineerd en geïntegreerd, zoals op sociale netwerksites als Hyves. En voor wie de informatie niet meer kan overzien is een zoekdienst als wieowie.nl die gecombineerd zoekt in Schoolbank, Flickr, LinkedIn, Youtube, Hyves, Google, etc. of diensten als Netvibes.com die gepersonaliseerde pagina's hosten met overzichtelijke RSS-feed informatie en andere webcontent.

Gebruikers delen dus auteursrechtelijke werken via filesharing, publiceren foto's of teksten op hun weblog of maken een video van professionele kwaliteit op Youtube. Het *clearen* van alle rechten is voor hen onbegonnen werk – voor zover ze al weten of vinden dat dit zou moeten. Hoe ga je daar als wetgever mee om? Creative Commons verplicht stellen? Collectieve licenties? Regelmatig wordt in dit verband de heffing op internetgebruik naar voren gebracht als middel om de auteursrechten te legaliseren.[23] Op de intellectuele eigendom, in het bijzonder het auteursrecht, wordt nader ingegaan in hoofdstuk 5.

Bij al de genoemde toepassingen wordt door de gebruikers al dan niet actief waardevolle (voor marketing, persoonlijk vermaak en informatiebehoefte, etc.) informatie verstrekt zonder duidelijke tegenprestatie. Het collectief van internetgebruikers lijkt zelfs in staat om de in vele jaren zorgvuldig opgebouwde Encyclopædia Britannica door de wat minder zorgvuldig opgebouwde Wikipedia van haar voetstuk te kunnen stoten.[24]

---

[22] Sector kanton rechtbank 's-Hertogenbosch 2 oktober 2008 (foto's), LJN BF9979, met noot Van der Linden, in: T. van der Linden-Smith & A.R. Lodder (2009), *Jurisprudentie Internetrecht Annotaties 2006-2009* (derde druk), Kluwer, Deventer.

[23] Zie onder andere 'Plasterk tegen heffing op internetgebruik', *Het Parool* 24 juni 2009 en 'FNV bepleit betaalde downloadlicentie als oplossing piraterij', *Tweakers* 18 januari 2010.

[24] R. van den Hoogen, A.R. Lodder & T. van der Linden, Inleiding, *Jurisprudentie Internetrecht*, Kluwer 2003.

Waarom stellen gebruikers schijnbaar vrijelijk al deze informatie ter beschikking? Op de Blog site Terra Nova (over virtuele werelden) is een van de categorieën om een bericht te kwalificeren "blatant selfpromotion". Minder populair kan worden gesteld dat een identiteit wordt gecreëerd waarbij de drijfveer erkenning door anderen is. Het controleren van verspreiding of het incasseren van royalty's is daaraan ondergeschikt of zelfs volstrekt irrelevant geworden. De erkenning vertaalt zichzelf naar inkomsten doordat men als persoon wordt ingeschakeld (dienstverlening) in plaats van dat voor het product wordt afgerekend. Maar lang niet altijd zit er zo'n model achter. De reden is dan vaak simpelweg "gewoon, omdat het kán".

De Amerikaanse AI & Law onderzoeker Ron Loui heeft bijvoorbeeld op zijn site[25] een aantal foto's en andere informatie geplaatst over contact dat hij in de loop der jaren met Barack Obama had, onder andere een e-mail uitwisseling over een te verzorgen Dinnerspeech tijdens het in St. Louis in 2001 georganiseerde internationale AI & Law congres (ICAIL).[26] Deze informatie is vooral voor de betrokkene (Ron Loui) interessant en zal voor de in Barack Obama geïnteresseerde weinig vermeldenswaardigs opleveren. Het illustreert wel de filosofie van Web 2.0. Het informeren van het publiek over zaken in je eigen leven die voor in ieder geval degenen die je kennen interessant kunnen zijn, maar voor de hele wereld toegankelijk zijn. De beschikbaarheid van zo veel informatie maakt het voor professionele media gemakkelijker om uit wat voorheen privé archieven waren materiaal te verkrijgen. Voor het bemachtigen van een klassenfoto van Barack Obama zou vroeger een zekere inspanning moeten worden geleverd, nu is deze eenvoudig op internet te vinden. Ook op de site van Ron Loui staat een klassenfoto met Barack Obama, waarover hij opmerkt dat ze *hem* (Ron Loui) nooit toestemming hebben gevraagd voor deze regelmatig in de krant gepubliceerde foto.

Een ander voorbeeld van een toepassing die vooral bedoeld is om te illustreren hoe interessant of belangrijk iemand is, is het zoge-

[25] http://www.cs.wustl.edu/~loui

[26] International Conference on Artificial Intelligence & Law, georganiseerd sinds 1987 door de internationale AI & Law vereniging IAAIL, zie http://iaail.org. Vermeldenswaard is dat Ron Loui als keynote speaker tijdens de in Parijs in 2006 georganiseerde JURIX-conferentie het publiek een boek liet zien van Barack Obama en zei dat hij bijna deze toekomstige president voor de in de hoofdtekst genoemde dinner speech had gestrikt. Weinig toeschouwers hadden op dat moment gehoord van Obama, die zoals bekend in 2009 inderdaad president van de Verenigde Staten van Amerika werd.

naamde Twitter en de daarbij behorende tweets.[27] Hierin geven mensen aan wat ze op een bepaald moment aan het doen zijn, wat ze van plan zijn te doen, waar ze zijn, etc. Tijdens het tot stand komen van de Wiki stond Twitter nog in de kinderschoenen, inmiddels is het een niet meer weg te denken Web 2.0 toepassing. Hiermee vergelijkbaar is het regeltje bovenaan het profiel in LinkedIn, waar de activiteiten (het lezen van een boek, het voorbereiden van een presentatie, etc.) kunnen worden vermeld. Ook zijn er deelnemers die via een in LinkedIn gebouwde 'Tripit' aangeven waar ze de komende tijd van plan zijn heen te reizen:

> See where your entire professional network is traveling and when you will be in the same city as your colleagues. Meet up at the next industry event or re-connect with old friends. Add the My Travel application to display your current location, upcoming trips and travel stats within your network.

In dit boek zal niet ingegaan worden op de op zichzelf interessante sociologische en psychologische vraag naar waarom al deze informatie op internet wordt geplaatst. We beperken ons tot de juridische merites.

1.3 Verschuivende grenzen: conducer? prosument?

Voor het recht heeft de democratisering van informatievoorziening grote gevolgen. Veel wetten en regelingen gaan uit van professionele informatieverstrekkers en dienstverleners tegenover consumenten. De consument wordt vaak beschermd ten koste van de dienstverlener. Een voorbeeld hiervan zijn de informatieplichten en het wettelijk recht op retour inzake overeenkomsten op afstand (artikel 7:46a e.v. BW). Deze afwijking van het beginsel van partijautonomie wordt gerechtvaardigd door het feit dat de producent veelal een professionele partij is met aanmerkelijk meer macht en mogelijkheden. Van deze professional mag verwacht worden dat hij de wettelijke vereisten binnen zijn bedrijfsvoering in ogenschouw neemt.

Andere wettelijke eisen, zoals die uit de Richtlijn elektronische handel (artikel 3:15d BW) gelden voor dienstverleners in het al-

[27] www.twitter.com

gemeen, niet alleen in de verhouding professional en consument. De vraag is welke regels van toepassing zijn op een consument die via Marktplaats.nl haar zelfgemaakte truien verkoopt? Moet een eigenaar van een profiel op een sociale netwerksite voldoen aan de informatieplichten van dienstverleners? Deze individuele gebruiker van een sociale netwerksite levert immers via zijn profiel op zijn beurt een informatiedienst. Een andere relevante vraag is in hoeverre de huidige wettelijke bescherming van de consument in de digitale wereld nog nodig is, of met andere woorden of door de opkomst van Web 2.0 de consument in sommige gevallen niet de sterkere partij is. Met de opkomst van Web 2.0 wordt op internet het onderscheid tussen de producent van informatie en de consument vager.

De term *prosument* verwijst naar de steeds actiever wordende consument. De toenemende activiteit onder consumenten wordt ondermeer veroorzaakt doordat het steeds makkelijker wordt een actieve bijdrage aan de markt te leveren, niet in de laatste plaats door de opkomst van vergelijkingssites als vergelijk.nl, kieskeurig.nl, snakewool.nl en de uit het internetrecht bekende El Cheapo.[28]

Consumenten kunnen met behulp van dergelijke sites een prijs- en kwaliteitsbewuste afweging maken tussen een groot aantal aanbieders. Voor producenten komt mede hierdoor nadruk te liggen op het vermogen zich te kunnen onderscheiden, bijvoorbeeld door zich steeds verder te professionaliseren en specialiseren, teneinde een betere service te kunnen leveren.[29]

De consument van weleer heeft echter steeds meer mogelijkheden om zelf te produceren. Hierdoor lijkt de scheidslijn tussen consumenten en producten te vervagen. De gemiddelde PC heeft nu tekst-, foto- en filmbewerkingssoftware waar de professionele studio uit de jaren tachtig alleen maar van kon dromen. Ook de mogelijkheden om werken en informatie te verspreiden zijn welhaast onbeperkt.

Wie heeft er niet een oom of een buurjongen die (al dan niet legaal) in CD's of DVD's heeft gehandeld, of een computerhobbyist

[28] Hoge Raad 22 maart 2002, LJN AD9138, R.H. van den Hoogen, A.R. Lodder & M. van der Linden-Smith (red.), *Jurisprudentie Internetrecht*, Kluwer 2003, p. 155-202 (met noot B.J. Lenselink).
[29] Zie ook J.E.J. Prins, *Bestaat de Prosument? Een verkenning naar consumenten- en producentenposities in de informatiemaatschappij*, 2001.

die van zijn hobby zijn beroep heeft gemaakt? Door dergelijke ontwikkelingen kan de oorspronkelijke aanpak van producenten, zijnde professionele partijen, een onbevredigende uitkomst opleveren bij een conflict.

Daarnaast zijn sites als Youtube, Flickr of MySpace manieren om jezelf dan wel 'jouw product/werk' aan de man te brengen. Ook zijn er consumenten die hun informatie delen middels weblogs. Vaak realiseren mensen zich echter niet dat je niet zomaar alles op voornoemde sites mag/kan aanbieden. Er kan bijvoorbeeld sprake zijn van strijd met het auteursrecht of portretrecht. Ook kan er sprake zijn van strijd met het industrieel eigendomsrecht wanneer bijvoorbeeld mensen merkproducten verkopen via voornoemde sites welke niet gekocht zijn via een legaal kanaal.

Veel wetgeving gaat uit van een zwart/wit model: de grote, professionele producent brengt werken en informatie op de markt, en de consument, een natuurlijk persoon die niet handelt in de uitoefening van beroep of bedrijf, neemt deze af. Vanuit dit model is bijvoorbeeld verdedigbaar dat de consument sterk beschermd wordt tegen de producent. Ook is het vanuit dit model redelijk dat een kopie voor eigen gebruik (artikel 16b Auteurswet) toegestaan is - dit doet een consument en daar heeft *dus* niemand last van.

Toch gaat veel wetgeving, en ook bijvoorbeeld de richtsnoeren van het CBP, nog steeds uit van een zwakke, onwetende consument die beschermd moet worden tegen kwaadwillende grote bedrijven. Indien de consument echter helemaal niet zo onwetend is als wordt gesuggereerd, schiet deze bescherming dan niet zijn doel voorbij? Probleem is echter om vast te stellen waar de grens loopt. Wie bepaalt wanneer een consument "onwetend", "goed geïnformeerd" of zelfs "deskundig" is?

Een eventuele gelijkschakeling tussen prosumenten en producenten zou er toe kunnen leiden dat de consument minder snel geneigd is om informatie in te winnen alvorens hij een overeenkomst aangaat, zodat hij bescherming blijft genieten. De wetgever probeert fundamentele belangen te beschermen. Is dit belang minder groot voor een consument die goed geïnformeerd is? Zal de goed geïnformeerde koper bijvoorbeeld niet even veel belang hebben bij een recht op correcte nakoming bij non-conformiteit (artikel 7:21 BW). Zelfs het feit dat de verkoper enigszins 'gelijkwaardig' is aan de consument lijkt hier niet veel aan af te doen.

Het gaat het bestek van dit boek te buiten om uitgebreid op het consumentenbeschermingsrecht in te gaan, maar het zal duidelijk zijn dat Web 2.0 het bestaande wettelijke regime in een nieuw daglicht plaatst.

1.4 Opbouw

Op de verschillende daarvoor bestemde internetpagina's (Hyves, Youtube, etc.) alsmede pagina´s met een ander doel die Web 2.0 functionaliteit hebben ingebouwd (bijvoorbeeld uploaden van reviews van boeken bij Bol.com) stellen internetgebruikers veelal grote hoeveelheden informatie ter beschikking zonder precies te weten:

- wat hun rechten zijn;
- welke rechten van anderen een rol spelen, en;
- welke rechten de beheerders van deze diensten zichzelf toemeten.

Via de wiki www.internetrecht20.nl is een aanzet gegeven tot het in kaart brengen van onderwerpen die relevant zijn voor Recht en Web 2.0. Op deze wiki zijn niet alle pagina's specifiek toegesneden op dit onderwerp, maar is ook voor het onderwerp relevante algemene informatie te vinden over bijvoorbeeld intellectuele eigendomsrechten of privacy. Op een wiki is deze achtergrondinformatie ondersteunend en kan indien er behoefte bestaat aan nadere toelichting worden geraadpleegd. Uiteraard is dergelijke algemene informatie in beginsel niet in dit boek opgenomen. Dit boek bevat een selectie van de "lemma's" die op de wiki te vinden zijn. Via de geschiedenis van iedere pagina kan worden vastgesteld wie welke informatie heeft toegevoegd. De bestaande teksten zijn wel nog waar nodig bewerkt. De reden dat dit niet in de wiki is gedaan, heeft ondermeer te maken met het ontbreken van een eenvoudige manier om de op een wiki aanwezige informatie in boekvorm om te zetten. Een andere reden is dat de wiki online moet worden geraadpleegd en ondanks de bestaande ontwikkelingen op het gebied van Cloud computing[30] is het internet niet altijd toegankelijk, zoals op het moment dat deze zin geschreven wordt.[31]

[30] De zeer geslaagde en bijzonder goed bezochte voorjaarsvergadering van de NVvIR, gehouden op 17 juni 2010, was aan dit onderwerp gewijd.
[31] Vlucht van Lissabon naar Amsterdam in mei 2009. Deze informatie is voor dit boek verder volstrekt oninteressant, hoewel het als illustratie kan dienen van een tweet.

In tegenstelling tot een boek, waar elke auteur zijn of haar eigen hoofdstuk tekst of onderdeel daarvan schrijft, kennen wiki's geen vaste auteurs. Iedereen kan elk stuk tekst aanpassen of uitbreiden, en nieuwe teksten toevoegen waar hem of haar dat goeddunkt. In het geval van *Recht en Web 2.0. Bewerkte bloemlezing uit www.internetrecht20.nl* kan dat ook nog nadat het boek gepubliceerd is. De wiki blijft open staan en kan naar believen worden aangepast. Als u het met bepaalde informatie niet eens bent, dan is het geheel in de geest van Web 2.0 mogelijk deze informatie aan te passen via www.internetrecht20.nl. Het boek moet veeleer als een verslag van een begin dan als een eindstation worden gezien. Daarbij bestaat de mogelijkheid om een groot aantal teksten in dit boek die nog niet op www.internetrecht20.nl te vinden zijn daar alsnog te plaatsen.

De bloemlezing die in dit boek is opgenomen[32] bestrijkt niet het volledige terrein van Recht en Web 2.0. Ook kunnen niet alle onderwerpen diepgaand worden geanalyseerd. Wat dit boek wel levert is een beschrijving van enkele belangrijke Web 2.0 diensten. Daarnaast worden aan de hand van diverse voorbeelden juridische vraagstukken die spelen toegelicht.

Na dit inleidende hoofdstuk wordt in hoofdstuk 2 nader ingegaan op een van de meest prominente toepassingen van Web 2.0, de sociale netwerksites. Na een algemene inleiding en bespreking van de belangrijkste kenmerken worden achtereenvolgens LinkedIn, Hyves, Facebook, Myspace en Orkut besproken. Bij iedere toepassing wordt niet enkel de toepassing zelf besproken, maar ook een of meer juridisch relevante voorvallen of kwesties. Afgesloten wordt met een paragraaf over risico en misbruik.

In hoofdstuk 3 worden enkele andere Web 2.0 toepassingen behandeld. Achtereenvolgens wordt ingegaan op File sharing (P2P), het delen van films en foto's, bloggen, microbloggen (Twitter), chat-sites en wiki-sites. Ook minder bekende toepassingen als social commerce en social bookmarking, alsmede calenders 2.0 en online geschillenoplossing 2.0 worden besproken. Tenslotte wordt ingegaan op de bij veel Web 2.0 toepassingen gebruikte Application Programming Interface.

In hoofdstuk 4 wordt kort ingegaan op virtuele werelden (uitgebreid behandeld in de NVvIR publicatie *Recht en Virtuele Werelden*

[32] Onder redactie van Arno R. Lodder en Rob van den Hoven van Genderen.

uit 2006), waarbij wordt aangegeven waarom deze tot Web 2.0 kunnen worden gerekend.

In hoofdstuk 5 worden enkele auteursrechtelijke kwesties behandeld. Binnen internetrecht in het algemeen een belangrijk onderwerp, maar voor Web 2.0 ook bijzonder relevant zijn de aan het up- en downloaden verbonden juridische consequenties. Met name enkele buitenlandse uitspraken over de Web 2.0 toepassing pur sang, P2P-programma's, worden besproken. Tenslotte wordt ingegaan op Creative Commons en embedded links.

In hoofdstuk 6 wordt de aansprakelijkheid zoals die vanuit het perspectief van de aanbieders in de algemene voorwaarden wordt geregeld besproken. De bijzondere positie van Web 2.0 bij aansprakelijkheid wordt vervolgens uitgewerkt aan de hand van de problemen waar aanbieders van discussieforums zich voor gesteld zien. Tenslotte wordt ingegaan op online veilingsites.

Een voor internet lastig vraagstuk is waar beslotenheid ophoudt en openbaarheid begint. In hoofdstuk 7 wordt hier dieper op ingegaan aan de hand van twee arresten van de gerechtshoven Den Bosch en Leeuwarden uit najaar 2009. Deze arresten handelden over de al dan niet openbaarheid van besloten Hyves-profielen.

In hoofdstuk 8 worden enkele privacy aspecten nader belicht. Ingegaan wordt op de richtsnoeren van de CBP voor gebruik van persoonsgegevens op internet, de zorgplicht van artikel 11 Wbp, hoe om te gaan met overleden Web 2.0 gebruikers, informatie bij sollicitaties, spam via krabbels, persoonlijke informatie van jongeren en de noodzaak tot bewustwording.

Het slothoofdstuk bouwt verder op de persoonlijke levenssfeer, maar dan vanuit het perspectief van degenen die tegen hun wil, onjuist of onrechtmatig genoemd worden op Web 2.0 sites, met name Hyves. Hierbij wordt uitgebreid op de rechtspraak op dit punt ingegaan.

2 Sociale netwerksites

Sociale netwerksites worden ook wel profielensites genoemd. Op deze sites plaatsen gebruikers informatie over zichzelf (een "profiel") in een gestructureerd formaat. Via uitnodigingen aan andere deelnemers wordt, na acceptatie van de uitnodiging, het eigen profiel gekoppeld aan het profiel van de ander. Op een sociale netwerksite kunnen gebruikers op deze manier contact leggen met mensen uit hun sociaal netwerk, maar dit ook uitbreiden door contacten aan te gaan met al dan niet willekeurige anderen. Voorbeelden van in Nederland populaire sites zijn Hyves en LinkedIn.[33] In onder andere de VS zijn Facebook en Myspace populair. Bij veel van deze profielensites beseffen gebruikers vaak beperkt dat deze informatie voor een wereldwijd publiek toegankelijk is. Ook dicht bij huis kan de geplaatste informatie gebruikt worden door minder gewenste bezoekers.

Zo werd in de zomer van 2009 door de politie gewaarschuwd niet op profielensites alsmede sites als Twitter informatie achter te laten over vakanties. Deze informatie wordt, niet geheel onverwacht, gebruikt door inbrekers. Waar in vroeger tijden ter plekke door bijvoorbeeld een met post volgestapelde deurmat deze informatie kon worden verkregen, maken sommige internetgebruikers het inbrekers gemakkelijk door geplande reizen te vermelden. Anderzijds is het in een online omgeving waar het de bedoeling is informatie te delen lastig om anderen niet te informeren over voorgenomen vakantieplannen of online op de hoogte te houden van belevenissen in al dan niet verre landen. Vooral voor de jeugd geeft de activiteit en zichtbaarheid op een sociale netwerksite een belangrijke bevordering van de sociale status.[34]

---

[33] Nederland is zelfs een van de landen met relatief en zelfs absoluut gezien een groot aantal LinkedIn gebruikers, reden waarom LinkedIn als locatie voor haar Europees kantoor Amsterdam koos. Zie 'LinkedIn opent kantoor in Amsterdam', *Het Parool* 22 september 2009. De daadwerkelijke opening van het kantoor vond plaats in januari 2010, zie *VKBanen*, 6 januari 2010 en 'Eerste Europese LinkedIn-kantoor opent in Amsterdam', *Computeridee* 6 januari 2010.

[34] Een zeer uitgebreid overzicht van de verschillende actoren op het internet, en de daar aanwezige sites wordt gegeven door Hanneke Vos en Arjan van Geel van Ruijgrok netpanel in *THE NEXT WEB 2009*, Amsterdam, 2009: http://www.ruigroknetpanel.nl/bestandenmap/RuigrokNetPanel_Onderzoeksrapport_NextWeb2009.pdf

Er bestaan verschillende soorten profielensites of sociale netwerksites. Er zijn sites die specifiek zijn toegesneden op een bepaalde doelgroep. De sites Sugababes.nl en Superdudes.nl richten zich bijvoorbeeld specifiek op tieners. Op Superdudes en Sugabes gezamenlijk zijn anderhalf miljoen profielen aangemaakt.[35] Op een andere populaire site voor jongeren CU2.nl, zijn een half miljoen profielen aangemaakt op de site.[36] Zoals wel vaker het geval is beperken de gebruikers zich niet tot de beoogde doelgroep, maar maken volwassenen met doorgaans weinig verheffende bedoelingen ook gebruik van dergelijke sites. Mede om die reden kwamen genoemde sites in 2006 negatief in het nieuws. Jeugdige gebruikers bleken informatie prijs te geven zoals telefoonnummers, huisadres, etc.

Een andere populaire doelgroep van sociale netwerksites zijn volwassenen die op zoek zijn naar een relatie. Een op grote schaal gebruikte site is Relatieplanet.nl. Op deze site presenteren de gebruikers zichzelf op een zo aantrekkelijk mogelijke manier voor toekomstige partners. Hoewel ongetwijfeld gebruikers van een op relaties gerichte site deze gebruiken om seksuele ontmoetingen te arrangeren, zijn er ook profielensites die zich expliciet hierop richten. Naast sites die zich richten op specifieke doelgroepen zijn er generieke sites waarvan in Nederland Hyves verreweg de bekendste is met meer dan 10 miljoen geregistreerde deelnemers.

Na een algemene karakterisering van sociale netwerken, zullen we kort enkele van deze meer algemene sites introduceren. Iedere paragraaf geeft algemene informatie over de sociale netwerksite en bespreekt een of enkele juridische casus of aspecten van de betreffende dienst.

2.1 Kenmerken

Het begrip sociaal netwerk is een fenomeen dat al zolang bestaat als er mensen interacteren. Een sociaal netwerk, dat in het spraakgebruik als 'netwerk' wordt aangeduid, is een netwerk van mensen of groepen mensen die elkaar kennen of via een verbindend element of eigenschap met elkaar in verbinding staan, of organisaties die vaak samenwerken. Dat kan op verschillende manieren, fysiek, elektronisch of virtueel.

[35] http://www.superdudes.nl/about en http://www.sugababes.nl/about
[36] http://www.cu2.nl/

In het verleden was er sprake van gemeenschappen waarin mensen met elkaar in verbinding stonden op basis van bepaalde eigenschappen en waar het nuttig en bevorderlijk werkte om de contacten onderling te bestendigen. Te denken valt hierbij aan de Gilden voor ambachtslieden of andere beroepsmatig met elkaar verbondenen. Ook op wetenschappelijk, ideologisch of filosofisch gebied zochten mensen elkaars nabijheid om ideeën uit te wisselen of andere delen van de samenleving te beïnvloeden. Naast bekende manifestaties van deze netwerken als politieke partijen en zeer grootschalige netwerken als religieus met elkaar verbondenen, kan ook worden gedacht aan bijzondere maar vaak hechte netwerken als de in de 17e eeuw opgerichte vrijmetselarij. De oorsprong hiervan zou liggen in de bescherming van de geheimen van de grootmeester metselaar van de bouw van de tempel van Salomon. Netwerk van recenter datum is de Rotary[37] met het kenmerkende netwerkwieltje.

De grondslag en doelstellingen van netwerken zijn variabel, zij het vaak gericht op het bereiken van een intensere samenwerking, humanitaire ontwikkeling en verspreiding van een bepaalde denkrichting van de verbondenen.[38] Dit soort netwerken maakt voor haar organisatie gebruik van een uitgebreid stelsel van (initiatie)rituelen en gedragsregels waaraan de deelnemers zich dienen te houden.

Vaak beoogt een netwerk een wederzijds voordeel, zoals het stimuleren van een bepaalde ontwikkeling, bewustwording van eigen kring, het wakker schudden van anderen of simpelweg economische belangen. Netwerken manifesteren zich niet altijd in het legitieme daglicht, denk hierbij aan de Cosa Nostra of Al Qaida die bestaan bij de gratie van de verbindingen tussen illegaal handelende individuen en ondergrondse activiteiten van organisaties.

In algemene zin behoren netwerken traditioneel tot een zelfde sociale laag, een "old boys" network of "peer group". Met name in het geval van de genoemde beroeps- of gildenetwerken, maar ook bij de vrijmetselarij, was hier sprake van. Ook bij wetenschappelijke netwerken en beroepsverenigingen is er sprake van informatie-uitwisseling tussen peer groups. Door de ontwikkeling van elektronische communicatienetwerken, internet is immers ont-

[37] Opgericht in 1905 met als credo het aanmoedigen van dienstvaardigheid.
[38] Zie voor een uitgebreid overzicht van de talloze (vaak Amerikaanse) genootschappen: http://www.stichtingargus.nl/vrijmetselarij/index2.html

staan uit de behoefte van de wetenschap om een mondiale uitwisseling van informatie te realiseren, hebben netwerken een belangrijke meerwaarde gekregen. Er kan meer en sneller informatie worden uitgewisseld.

De peer-group netwerken van de eerste generatie worden de laatste jaren door het gebruik van elektronische verbindingen en semi-anonimiteit meer en meer aangevuld door contactnetwerken uit verschillende sociale lagen en deelnemers met een verschillende beroepsachtergrond met een grote variatie aan specifieke deelbelangen. Bij de elektronische sociale netwerken is vooral het, virtuele of online, contact belangrijk geworden.

2.1.1 De moderne sociale netwerken sites

De elektronische sociale netwerken zijn zeer variabel in hun doelstelling en deelnemers. Sociale netwerksites bestrijken inmiddels het gehele spectrum van sociale, maatschappelijke en meer professionele activiteiten. WG 29, de werkgroep van privacy toezichthouders, houdt de volgende definitie aan van sociale netwerksites (Social Networking Sites of SNS):

> *SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users*.[39]

Afhankelijk van de doelstelling van een sociale netwerksite en zijn beoogde deelnemers, kan de geboden functionaliteit enigszins variëren. In het algemeen kunnen de volgende kenmerken en eigenschappen worden onderscheiden:[40]

- De gebruikers verstrekken hun kenmerken (profiel) om contacten te genereren, het profiel is het basisinstrument voor verdere activiteiten;
- De SNS voorziet in een mechanisme om profielen te personaliseren door een veelsoortige productie van "user generated content", in de vorm van allerlei bestanden, films, foto's, tekstbestanden, links, etc.;
- Er is een communicatiemogelijkheid via mail, chat-sessies, electronic bulletinboard, etc.;

[39] Opinion 5/2009 on online social networking, 01189/09/EN WP 163 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf
[40] Uitwerking van enkele kenmerken als aangegeven in opinion5/2009 WG 29 (zie noot 39), p. 5.

- Het is mogelijk contacten toe te voegen in eerste, tweede of derde graad waarbij een soort kettingbriefprincipe kan worden gebruikt om verdere uitbreiding van de vriendenkring te realiseren;
- De SNS voorziet in advertenties die zijn gerelateerd aan het gegenereerde profiel (targeted advertisements), hoewel ook diensten tegen betaling kunnen worden geleverd, zoals extra contactmogelijkheden, een verbeterde profielweergave of zelfs het *niet* tonen van advertenties.

2.1.2 Onderverdeling SNS

Op basis van de doelstellingen van de SNS kan een volgende indeling worden gemaakt:

a) sociaal algemene (relatie) netwerken als Hyves, Facebook en Myweb;
b) professionele netwerken als LinkedIn en;
c) gespecialiseerde relatienetwerken als schoolbank, dienstmaatjes, etc.

Er is inmiddels duidelijk een trend waarneembaar van een algemene oriëntatie van de SNS naar een meer gespecialiseerde, doelgerichte ontwikkeling.[41] Inkomsten van de SNS worden niet alleen meer gehaald uit de "naastliggende" commerciële advertenties, maar ook wordt steeds vaker een financiële vergoeding gevraagd aan de deelnemers van het netwerk. Dit is vaak een geleidelijk proces. In eerste instantie wordt het netwerk gratis aangeboden. Na een bepaalde periode, meestal als er inmiddels een aanzienlijke contactenkring is opgebouwd, wordt de deelnemer verwittigd van het feit dat als hij in de toekomst wil blijven gebruikmaken van de SNS helaas een kleine vergoeding moet worden gevraagd. Aangezien men zijn contacten niet wil verliezen is het opzeggen van deze betaaldienst dan onaantrekkelijk.[42] De SNS aanbieder zal zich vervolgens moeten realiseren dat het aanbieden van diensten tegen vergoeding verplichtingen met zich mee brengt die verder reiken dan in het geval van gratis diensten.

[41] Een trend van SNS is "the shift from Web 2.0 for fun to Web 2.0 for productivity and services". Speech *Internet of the future: Europe must be a key player* van Vivian Reding, European Commissioner for Information Society and Media tijdens de bijeenkomst *Future of the Internet* initiative of the Lisbon Council, Brussels, 2 February 2009.

[42] In 2010 kondigde sociale netwerksite NING aan dat ze haar dienst van een gratis naar een betaaldienst om zou zetten. Dit leverde een storm van protest op onder gebruikers, vaak afkomstig uit de nonprofitsector. Zie <http://blog.ning.com/2010/04/an-update-from-ning.html>

2.2 LinkedIn

LinkedIn is een zakelijke, sociale netwerksite die actief is sinds mei 2003, en gericht is op professionals. Nederland is één van de meest intensieve gebruikers (meer dan een miljoen deelnemers). Daarom werd begin 2010 in Nederland een kantoor geopend op de Amsterdamse Zuidas. In tegenstelling tot bijvoorbeeld de sociale netwerksites die puur op de sociale ontwikkeling van (de vriendenkring van) haar gebruikers zijn gericht, zoals Hyves, ligt de focus van LinkedIn meer op functionaliteit. Dit neemt niet weg dat op menig profiel vrienden, bekenden en familie te vinden zijn. De grenzen zijn hierbij overigens niet scherp te trekken, want in de regel is het ook in een professioneel netwerk interessant om banden met niet uit de directe werksfeer komende contacten te onderhouden.

2.2.1 Risico's gratis dienst

Gebruik maken van LinkedIn is in beginsel gratis, maar extra functionaliteiten worden geboden indien een betaalde dienst wordt afgenomen. Het gros van de gebruikers beperkt zich tot de gratis dienstverlening. Er schuilt een zeker risico in het intensief gebruiken van een dergelijke gratis dienst. Zo vermelden de voorwaarden dat ieder moment de diensten kunnen worden gestopt. De kans daarop is niet heel groot, maar hoe meer informatie je in het netwerk stopt, hoe groter de schade zal zijn als de dienst onverhoopt niet meer aangeboden wordt. Het voor de zekerheid parallel aan LinkedIn bijhouden van vergelijkbare gegevens (zoals de adresinformatie) kan natuurlijk, maar de toegevoegde waarde van LinkedIn wordt daarmee navenant minder.

Ook zou het kunnen dat LinkedIn op enig moment de dienst niet meer gratis zal aanbieden. Op het internet is het doorgaans geen groot succes als een dienst tegen betaling wordt aangeboden die

eerder gratis was, maar uit te sluiten dat dit gebeurt is het zeker niet. Er wordt door LinkedIn flink geïnvesteerd in de site en als bijvoorbeeld de advertentie-inkomsten zouden teruglopen kan er een moment komen dat de bestaande dienst niet langer rendabel is en zal er een keuze gemaakt moeten worden. Een dergelijke wijziging zal meer nog dan de individuele gebruiker de zogenaamde LinkedIn groepen treffen. De Nederlandse Vereniging voor Informatietechnologie en Recht maakt hier gebruik van,[43] maar heeft daarnaast nog steeds haar klassieke ledenbestand. Er zijn echter groepen die zich gevormd hebben via LinkedIn en alleen daar als groep bestaan. Voor deze groepen zal een beleidswijziging van LinkedIn bijzonder ingrijpend kunnen zijn.

Eén van de door de aanbieder gepropageerde voordelen van LinkedIn is dat door het doorverwijzen via vertrouwde gemeenschappelijke contacten of door een van tevoren al bestaande relatie vertrouwen ontstaat tussen de deelnemers aan het netwerk. Een kleine steekproef leert echter dat het vrijwel nooit voorkomt dat iemand zich als connectie aandient zonder de benaderde persoon te kennen of tenminste bekend te zijn met een gemeenschappelijke belangstelling. Waar in de offline wereld bij gelegenheden nog wel eens iemand zichzelf introduceert of het gesprek opent bij een hem niet persoonlijk bekende met het noemen van een gezamenlijk contact, lijken deelnemers zich voor zover ons bekend vrijwel nooit met een dergelijke introductie als mogelijke connectie te melden. Het is ook niet duidelijk wat de waarde van een dergelijk indirect contact verder is, behalve dat personen die graag zoveel mogelijk contacten willen hebben uiteraard elke mogelijkheid zullen aangrijpen.

2.2.2 Relatiebeheer

Het primaire doel van een site als LinkedIn is – behalve online vermaak - het systematisch leggen en onderhouden van contacten. Het Web 2.0 element bestaat er deels uit dat iedereen kan meegenieten van mededelingen over gewijzigde profielen, de nieuwe contacten die zich binnen een bepaalde voorafgaande periode bij personen uit je netwerk hebben gemeld, etc. Een ander belangrijk aspect van LinkedIn is dat de contactinformatie wordt bijgehouden door de contacten zelf. Anders dan in normale adresboeken het geval, hoeft de gebruiker daarvan dus niet iedere wijziging, verhuizing of verplaatsing te verwerken, maar wordt dit voor hem gedaan. Dit scheelt, zeker als er een groot netwerk on-

[43] http://www.linkedin.com/groups?gid=82244&trk=myg_ugrp_ovr

derhouden moet worden, veel tijd. Essentieel is daarbij wel dat de gebruikers hun informatie ook daadwerkelijk bijwerken. Dit lijkt vooralsnog het geval te zijn, maar kan uiteraard in de toekomst veranderen.

Er zijn deelnemers die hun belang (lijken te) ontlenen aan het aantal contacten dat ze hebben. LinkedIn probeert zelf te benadrukken dat het om de kwaliteit van de contacten moet gaan en niet om de kwantiteit. Indien iemand duizenden contacten heeft, neemt het belang van dit persoonlijke netwerk inherent af. Er zijn ook mensen die om die reden afhaken, zoals de oprichter van XS4ALL Rop Gonggrijp:[44]

> "With LinkedIn came the hundreds of invitations, some of people I didn't know at all. The awkwardness of thinking about whether to accept or reject an invitation, multiplied by at least one such awkward invitation a week just got me thinking…
>
> What has LinkedIn done for me lately? It has caused me work, and awkward cringes and it has given, well, absolutely nothing in return.
>
> So, I just cancelled my account (which needs to be done by emailing customer support). I'll cancel my Hyves and Orkut accounts too, since I never log in there anymore."

2.2.3 Oplichting

Los van al dan niet aan het gebruik van LinkedIn verbonden voordelen is mogelijk misbruik de keerzijde van het publiekelijk ter beschikking stellen van allerhande persoonlijke informatie.

In de zomer van 2008 hadden West-Afrikaanse oplichters LinkedIn ontdekt.[45] Zij stuurden mails rond met valse informatie om op deze wijze bank en privé gegevens van mensen te bemachtigen (phishing) zodat deze vervolgens beroofd konden worden. Eén van

[44] http://rop.gonggri.jp/ Het in de hoofdtekst aangehaalde bericht komt uit 2008. In maart 2010 meldde Gonggrijp op zijn blog dat hij zich bij Facebook had aangemeld, omdat dit een onmisbaar instrument is om mensen politiek te motiveren, organiseren en campagnes te voeren, zie *Wie is U?* van Karin Spaink e.a (2010), p. 24-25. De blogposting is van 22 maart en opent met: "As I slowly shake off the winter and re-enter communications mode I joined Facebook yesterday, after dramatically saying goodbye to all social networking two years ago."

[45] http://webwereld.nl/articles/51217/sophos--oplichters-misbruiken-linkedin.html

de redenen dat de West-Afrikaanse oplichters gebruikmaakten van LinkedIn, is vermoedelijk dat de gebruikers van de netwerksite relatief rijk zijn:

> "419 scammers may be hoping that the typical professional on LinkedIn may have more disposable income than the archetypal MySpace or Facebook user, and is potentially a bigger catch.",

aldus Graham Cluley, senior technology consultant van Sophos.[46]

Daarnaast stellen Web 2.0-sites zoals LinkedIn oplichters in staat om spamfilters van bedrijven te omzeilen. Dit laatste lijkt medio 2010 lang niet altijd het geval. De server van de Vrije Universiteit bezorgt bijvoorbeeld standaard allerhande via LinkedIn geposte berichten van netwerkcontacten in de SPAM-box.

2.3 Hyves

De in 2004 opgerichte sociale netwerksite is in Nederland verreweg de populairste met meer dan 10 miljoen geregistreerde gebruikers. Er wordt veel informatie via deze site uitgewisseld, op een willekeurige dag in juni 2010 bijvoorbeeld:

- 418.389 Krabbels vandaag;
- 9.066 Blogs vandaag.

[46] http://www.sophos.com/pressoffice/news/articles/2008/05/linkedin.html

2.3.1 Politici en lijsttrekkersdebat

Politici zijn en waren ook actief op deze sociale netwerksite. Op 2 juni 2010 vond zelfs een lijsttrekkersdebat op Hyves plaats. Voorafgaand aan het debat was het mogelijk via een poll een thema voor het debat te kiezen. De vier meest gekozen thema's zijn op 2 juni 2010 besproken door de politici via de Hyves chat. De politici gingen per koppels van twee in debat en waren te volgen via een speciale pagina.[47] Na de discussie konden de Hyves-gebruikers de in hun ogen beste lijsttrekker kiezen.[48] Vrijwel alle lijsttrekkers deden mee, onder andere Jan Peter Balkenende, Femke Halsema, Emile Roemer, Mark Rutte, Alexander Pechtold en Job Cohen. Uiteindelijk bezochten 50.000 Hyvers de chat pagina. Als winnaar kwam Mark Rutte (28%) uit de bus, gevolgd door Emile Roemer (20%) en Femke Halsema (16%).

De profielen van bekenden zoals politici zijn speciaal ingesteld zodat meer vrienden dan bij een regulier profiel zich kunnen melden. Door je aan te sluiten als vriend van een bepaalde politicus, maak je kenbaar waar je politieke voorkeur naar uitgaat. Deze informatie valt onder gevoelige gegevens in de zin van de Wbp, maar wordt niettemin achteloos op de sociale netwerksite achtergelaten. Op het moment dat iemand ook meer dan tientallen of hooguit honderden vrienden heeft, kan deze vriendenschare al eigenlijk niet meer dienen om iets over je eigen vriendenkring aan anderen te melden (anders dan dat je er veel hebt), daar is hij eenvoudig weg te groot voor.

Balkenende kan meer dan drie keer de Arena laten vollopen met alleen maar Hyves-vrienden,[49] die als groep herkenbaar zijn maar individueel niet vindbaar zijn op de pagina van Balkenende. Op de profielsite van de vrienden van Balkenende daarentegen is gemakkelijk te zien dat ze vriend van Balkenende zijn. Als de uitnodiging om vrienden te worden door een bekende Nederlander wordt geaccepteerd zegt dit uiteraard niets over zijn vriendenkring, maar maakt dit enkel duidelijk wie zijn 'vrienden' zouden willen zijn.[50] Het is een goede illustratie van de gedachte achter Web 2.0, dat je vooral over jezelf vertelt.

[47] http://hyves.nl/chatdebat
[48] www.hyves.nl/verkiezingen
[49] Begin juni 2010 had hij meer dan 200.000 vrienden.
[50] Zoals onlangs een meisje van 8 tegen een meisje van 7 zei: „Heb jij Hyves? Op Hyves is Paul de Leeuw mijn vriend en die is heel beroemd."

2.3.2 Politie

In de zomer van 2008 meldde de Amsterdamse politie dat ze netwerksites zouden gaan onderzoeken. Het ging hier om het via sociale netwerk analyse, een aparte sub-discipline binnen zowel sociologisch onderzoek als de informatica, in kaart brengen van criminele netwerken. Met behulp van speciale software, zoals data-mining en profiling technieken, kan de grote hoeveelheid op Hyves beschikbare informatie geanalyseerd worden. Op deze wijze kan door het in kaart brengen van de bij een crimineel aangesloten 'vrienden' inzicht gekregen worden in een mogelijk crimineel netwerk. Een moeilijkheid bij dit type onderzoek is echter dat steeds meer 'hyvers' hun profiel alleen toegankelijk maken voor vrienden. De politie mag, omwille van de privacy, niet inbreken op een profiel om informatie te verkrijgen. Hierdoor zullen gesloten profielen veelal buiten het onderzoek vallen. De technieken kunnen dus niet preventief gebruikt worden, maar zodra iemand als verdachte wordt aangemerkt (en bij terrorisme al eerder)[51] bestaat de mogelijkheid dat deze in beginsel besloten informatie toch doorzocht wordt.

Begin 2010 maakte de Politie Noord Limburg bekend dat ze sociale netwerken intensiever willen gebruiken om misdaden op te lossen.[52] Zo is de Politie Noord Limburg te vinden op Twitter[53] en op Hyves.[54] Ook houdt de politie een weblog bij tijdens het programma Opsporing Verzocht. De recherche geeft bezoekers via de sociale netwerksites inzicht in gegevens uit lopend onderzoek, in de hoop zo meer tips van burgers te krijgen.

Niet alleen criminelen laten op Hyves mogelijk voor henzelf nadelige informatie achter, ook de opsporingsambtenaren zelf zijn niet al te zorgvuldig:[55]

> "De politie wil graag boeven vangen met behulp van Hyves, maar zou er vooral goed aan doen de berg aan privacygevoelige gegevens van eigen dienders op netwerksites te beteugelen."

[51] Denk hierbij aan de speciale bepalingen in het Wetboek van Strafvordering inzake terrorisme.
[52] *Tijdschrift voor Internetrecht 2010/2*, Signaleringen.
[53] http://twitter.com/politieln
[54] http://politie-lbn.hyves.nl
[55] http://webwereld.nl/articles/51568/-politiemensen-zetten-te-veel-priv--info-op-hyves-.html

Voorgaande quote komt uit een artikel over dat de politieleiding te weinig doet om personeel ervan bewust te maken dat het achterlaten van privé-informatie op internet onverstandig is. Alleen al op Hyves zijn meer dan vijfduizend profielen (inclusief foto's) te vinden van politiemedewerkers. Ook op sites als Facebook, Partyflock, Sugababes en LinkedIn zijn veel privégegevens van Nederlandse politiemensen te vinden. Voormalig rechercheur Van Roij stelt:

> "Op deze sites maakt de Nederlandse diender er geen geheim van dat hij bij de politie werkt, wat zijn functie is, of hij getrouwd is, hoe zijn kinderen heten en waar ze op school zitten. Het is zelfs helemaal niet moeilijk om te achterhalen wanneer iemand op vakantie gaat en waar het gezin naar toe gaat."

Behalve deze betrekkelijk triviale informatie is er ook ronduit gevoelige informatie op Hyves terug te vinden:

> "Een klein onderzoek in voor een ieder zichtbare krabbels op Hyves legt al snel bloot wanneer een politieman nachtdienst heeft of in welk Team Grootschalig Optreden hij werkzaam is."

Dergelijke onvoorzichtigheid zal vermoedelijk afnemen zodra mensen zich bewust worden van de impact die dergelijke achteloos achtergelaten informatie kan hebben. Het blijft niettemin lastig om in een omgeving, waar op basis van al dan niet virtuele vriendschappelijkheid informatie wordt uitgewisseld, steeds bewust te blijven van de mogelijke consequenties.

2.3.3 Hacken account

Het kan ook voorkomen dat er informatie op een site wordt geplaatst die niet door de eigenaar van het profiel daar is neergezet. Anderen kunnen commentaar leveren via zogenaamde krabbels of een profiel aanmaken van een ander persoon. Ook kan er worden ingebroken op een profiel. Dit overkwam Huub van Ballegooy, een van de bewoners van de Gouden Kooi.[56] Op zijn profielsite werd vermeld dat hij op zoek was naar een leuke vent. Hij zou naast zijn vrouw ook wel graag een fijne man hebben. Op zichzelf geen schokkende onthulling, behalve dus dat deze Huub dat niet zelf had aangegeven. De reactie van deze Hyver is, hoewel ongetwij-

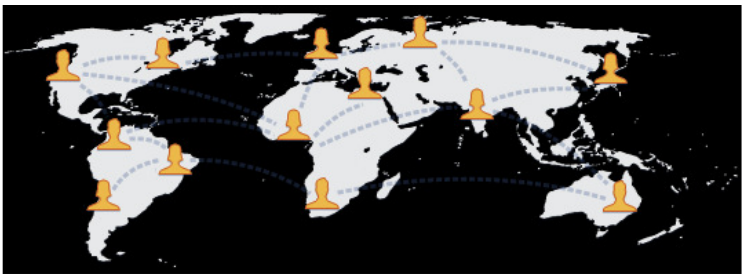
[56] http://www.medianed.com/2008/10/08/gouden-kooi-huubs-hyves-gehackt/

feld in geëmotioneerde toestand gedaan, voor de doorsnee Nederlander schokkender dan de `ludieke´ onthulling:

> ""een of andere sneaky motherfucker of motherfuckster heeft mijn hyves gejat! (..) Ze moeten degene die dit gedaan heeft eerst stokslagen op de voetzolen geven geven, kaalscheren en op een platte kar door het dorp heen rijden…en tot bloederig slot daarna ongeblindoekt executeren….met hagel!"[57]

2.4 Facebook

Facebook is een internationaal georiënteerde profielensite vergelijkbaar met het Nederlandse Hyves.



2.4.1 Beacon en privacyinstellingen

Medio 2008 is Facebook aangeklaagd voor het schenden van online privacy van de gebruikers en het overtreden van computerfraudewetgeving. Reden voor de aanklacht is het controversiële 'Beacon' systeem. Met Beacon werd de activiteit van Facebookgebruikers bijgehouden en getoond aan andere bezoekers van de site. Zo kunnen Facebook vrienden zien welke sites je hebt be-

[57] Gepost op een niet langer toegankelijke BLOG-site.

zocht en welke producten je (online) hebt gekocht. Dit werd door veel gebruikers ervaren als een privacyinbreuk. In de aanklacht werd gesteld dat Facebook informatie over het surfgedrag van zijn gebruikers verzamelde en verspreidde zonder goedkeuring van de gebruikers. De aanklacht beslaat de periode van 7 november 2007 tot en met 5 december 2007, na deze datum werd het voor gebruikers mogelijk om Beacon helemaal uit te zetten en eind 2009 werd de service uiteindelijk afgesloten.

In december 2009 werden de privacyinstellingen aangepast, hetgeen volgens Facebook moest leiden tot betere waarborgen. Vreemd genoeg resulteerde dit erin dat gegevens die gebruikers als privé hadden ingesteld, openbaar werden voor alle Facebookgebruikers.[58]

In juni 2010 had Facebook de instellingen wederom aangepast, waardoor het mogelijk is om op een centrale plaats op de site aan te geven voor wie welke gegevens toegankelijk zijn.[59] De elektronische burgerrechtenbeweging EFF is hier tevreden mee, maar richt zich via een open brief op een aantal resterende problemen:[60]

> "We are glad to see that Facebook has taken steps in the past weeks to address some of its outstanding privacy problems. However, we are writing to urge you to continue to demonstrate your commitment to the principle of giving users control over how and with whom they share by taking these additional steps: (…)"

Het gaat daarbij onder andere om het verbeteren van de "app gap" waardoor gebruikers de mogelijkheid krijgen te beslissen welke toepassingen toegang krijgen tot hun persoonlijke informatie en de "instant personalization" opt-in maken.

---

[58] T. van der Linden & T. Wisman (2010), *Image-building op het internet: houd greep op je digitale* identiteit, Rapport in opdracht van opdracht van SURFdirect, de DIgitale Rechten Expertise Community van SURF, zie http://www.surffoundation.nl/SiteCollectionDocuments/SURFdirect_Image-building_op_het_internet_mrt2010_DEF.pdf.

[59] http://www.nu.nl/internet/2271965/privacyclubs-willen-meer-aanpassingen-van-facebook.html

[60] http://www.eff.org/press/archives/2010/06/16, de volledige tekst is te vinden via http://www.eff.org/files/filenode/social_networks/OpenLettertoFacebook.pdf

2.4.2 Applicaties van derden

Een aardige uitbreiding van sociale netwerksites is het bieden van de mogelijkheid om applicaties van derden toe te voegen. Het kan hierbij gaan om onschuldige toepassingen als het laten zien van Youtube filmpjes, foto's van Flickr of andere innovatieve – al dan niet Web 2.0 – toepassingen. Een dergelijke functionaliteit biedt eveneens mogelijkheden aan spammers en andere kwaadwillenden. Zo werd in het najaar door een groep onderzoekers gewaarschuwd voor een omstreden Facebook-plugin die websites plat kon leggen. Dit werd gedaan door een op het eerste oog onschuldig programmaatje "photo of the day", dat enkel tot doel lijkt te hebben om dagelijks een nieuwe foto van national geographic te laten zien. Op de achtergrond draait echter een onzichtbaar proces dat er voor zorgt dat er bij elke klik een HTTP-aanvraag van 600 Kb naar de website van een slachtoffer wordt gestuurd.[61] Nader onderzoek wees uit dat dit kan leiden tot een data load van 23 Mb per seconde, omgerekend zo'n 248 Gb per dag. Daarmee kan het een website platleggen, vergelijkbaar met een DDoS-aanval.

Een ander hiermee samenhangend probleem is dat Facebook-applicaties toegang hebben tot persoonlijke gegevens van gebruikers, dus het is eenvoudig om deze te verzamelen en te versturen naar een afzonderlijke server. Platformontwikkelaars die deze applicaties maken moeten een contract ondertekenen waarin ze aangeven dat ze de privacyinstellingen van de gebruikers respecteren en waarin de verzameling van persoonlijke gegevens aan banden wordt gelegd. Facebook geeft aan dat ondanks dit contract en technische voorzorgsmaatregelen, er vormen van misbruik van persoonlijke gegevens kunnen plaatsvinden. Daarnaast kunnen platformontwikkelaars voorwaarden opstellen die de gebruiker van de applicatie moet accepteren en waardoor de ontwikkelaars meer rechten krijgen over de persoonlijke gegevens.

2.5 My space

In 2004 maakte MySpace de overgang van virtuele opslagruimte naar sociale netwerksite.

[61] http://www.ics.forth.gr/~elathan/publications/facebot.isc08.pdf

2.5.1 Leeftijdsgrenzen

Om een eigen profiel op MySpace te kunnen maken moet je minimaal 14 jaar zijn.[62] Als je nog geen 16 bent is je profiel automatisch alleen voor privé contacten beschikbaar. De onderhouders van de site zijn heel actief in het bestrijden van elke vorm van ongewenste informatie-uitwisseling. In juli 2007 hebben zij 29.000 profielen, die toebehoorden aan personen die zich schuldig hadden gemaakt aan vormen van seksueel misbruik, van de site verwijderd.

2.5.2 Cyberpesten

In de zomer van 2008 werd een vrouw aangeklaagd en ervan beschuldigd dat zij een meisje van 13 jaar (haar buurmeisje) via MySpace zo erg had gepest dat het meisje zelfmoord pleegde. Hier werd de vraag gesteld of de Amerikaanse cybercrime wetgeving ook kon worden toegepast in het geval van zogenaamd 'Cyberpesten'. MySpace gaf aan tegen cyberpesten te zijn en volledig mee te werken aan het voor de zaak noodzakelijke onderzoek.[63]

De dader, Lori Drew, werd vervolgd op grond van de *Computer Fraud and Abuse Act*. In eerste instantie werd ze veroordeeld, vanwege het gebruik van een valse identiteit. Deze veroordeling in 2008 werd in hoger beroep in 2009 teruggedraaid. De moeder van het slachtoffer was daar om begrijpelijke redenen niet tevreden mee:[64]

[62] Zie ook paragraaf 8.6 over leeftijdsgrenzen bij persoonlijke informatie op sociale netwerksites.
[63] Zie http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier en *Als 49-jarige bijdragen aan het "doodpesten" van een 13-jarige. Manslaughter? Murder in the 1st or 2nd degree?*, http://jurel.nl/2008/08/15/
[64] Celizic, Mike (July 3, 2009), "MySpace Victim's Mom Disappointed by Ruling," TODAY MSNBC.com, http://today.msnbc.msn.com/id/31722986/ns/today_people

> "I think it needed to let people know: You get on the computer, you use it as a weapon to hurt, to harm, to harass people, this is not something that people can just walk away from. This is many times the teen's lifeline."

2.6 Orkut

Orkut is in januari 2004 gelanceerd door zoekmachine-fabrikant Google en genoemd naar een van haar medewerkers, Orkut Buyukkokten.[65]

2.6.1 Deelnemen via uitnodiging

Aanvankelijk kreeg je alleen toegang tot Orkut via een uitnodiging van iemand die al deelnemer was. Deze procedure was eerder ook in gebruik bij de mail-service van Google, gmail en begin 2010 wederom in zwang bij de Wave van Google. Gevolg van deze strategie bij Orkut was dat deelnemers aan anderen die graag toegang wilden tot het netwerk geld vroegen. Het is duidelijk dat de strategie die hierachter schuilt, een zekere exclusiviteit, niet meer werkt als tegen betaling ook zonder bekende gebruikers toegang kan worden gekregen. Inmiddels is deze werkwijze al geruime tijd afgeschaft, iedereen kan zich aanmelden bij Orkut. Orkut is vooral populair in Brazilië en India.

2.6.2 Regels moederbedrijf Google

Indien je aan Orkut wilt deelnemen heb je een Google account nodig. Dit houdt in dat de voorwaarden die Google aan haar accountdeelnemers stelt voor alle deelnemers van Orkut gelden. Hier komen allerlei juridische aspecten bij kijken. Een voorbeeld is dat Google je via Orkut verstrekte persoonlijke gegevens en de inhoud van je communicatie verwerkt en onderhoud. Verder wor-

[65] http://www.nytimes.com/2007/11/04/technology/04digi.html?ref=business

den deze gegevens gebruikt voor doeleinden beschreven in het privacybeleid van Google.

In het privacybeleid van Google staat onder andere dat je persoonlijke gegevens gebruikt kunnen worden voor controle, onderzoek en analyse om de Google technologieën en –services te leveren en te verbeteren. Hiernaast is er bepaald dat Google gecombineerde, niet traceerbare gegevens aan derden mag geven. Verder kan in speciale gevallen ook aan derden gegevens ter beschikking worden gesteld, als hierdoor in overeenstemming met juridische procedures, fraude of schade kan worden voorkomen of het de veiligheid van het netwerk garandeert.

2.6.3 Beledigen docent

De rechtbank van Rondonia (Brazilië) heeft in 2008 een zaak gewezen met betrekking tot Orkut. In deze zaak heeft de rechter negentien jongeren veroordeeld tot betaling van schadevergoeding voor de morele schade die zij hadden veroorzaakt bij een wiskunde docent omdat zij hem hadden beledigd in Orkut. De rechter hield uiteindelijk de ouders van de jongeren verantwoordelijk, omdat zij hun verplichting om goed op hun kinderen te letten niet waren nagekomen.

2.7 Risico's en misbruik

Vaak is het de gebruiker niet duidelijk welke regels van toepassing zijn op de deelname aan de sociale netwerksite. De gebruiker is, bij zoveel diensten die via internet worden aangeboden, geneigd om simpel het kruisje te zetten in het icoontje "aanvaarden van de algemene voorwaarden" zonder die daadwerkelijk gelezen te hebben, laat staan te begrijpen in hoeverre de algemene voorwaarden ruimte geven aan andere partijen om de gegenereerde inhoud en persoonlijke informatie te benutten, aan te passen of te verspreiden. Deze "click through" of "clikwrap"-overeenkomsten zijn inmiddels aanvaard, maar net als in de offline wereld weet de gebruiker doorgaans niet waaraan hij zich bindt.

2.7.1 Gevolgen deelnemen

De voorwaarden van LinkedIn wijzen op de vergaande gevolgen van het openen van een account:

> By accessing, viewing, downloading or otherwise using LinkedIn or any webpage or feature available through LinkedIn, any information provided as part of the LinkedIn services, or any related emails, newsletters or services (hereinafter collectively "LinkedIn" or the "Services"), or by clicking "Join LinkedIn" during the registration process, you conclude a legally binding agreement with LinkedIn Corporation

Ook is een bepaling opgenomen waarin de toekomstige gebruiker wordt gewaarschuwd slechts weloverwogen een beslissing over het openen van een account te nemen:

> Prior to joining LinkedIn, you must consider and decide, yourself, the extent to which you wish to reveal information about yourself to the large community of LinkedIn Users and to LinkedIn and you must not communicate to LinkedIn and its Users any information the dissemination of which could be harmful to you.

In het licht van het feit dat voorwaarden over het algemeen amper bekeken worden, draagt een dergelijke bepaling niet bijzonder bij aan een bewuster gebruik van de dienst.

2.7.2 Misbruik

De risico's van het gebruik van sociale netwerken zijn voor de hand liggend, maar worden door de gebruikers niet altijd even serieus genomen. Die risico's kunnen ontstaan door naïviteit, het ontbreken van inzicht in de mogelijkheden van gebruik van het profiel door de aanbieder van de sociale netwerksite, eigen onzorgvuldigheid in de presentatie van informatie, maar in toenemende mate ook door misbruik door derde partijen. Op dit soort sites geeft men gevoelige informatie prijs die met genoegen wordt geconsumeerd door partijen die hier gebruik en misbruik van willen maken, zoals ook in de voorgaande paragrafen verschillende keren naar voren kwam. Niet alleen kan deze informatie worden benut door de medegebruikers van dit netwerk, maar ook door de host-organisatie, overheid, werkgevers, commerciële derden en criminelen. De persoonlijke informatie die zich op de "account" bevindt is een waardevolle resource die kan worden geëxploiteerd. Een bewustwording van die gevaren is essentieel voor elke deelnemer aan sociale netwerksites.

De verwachting is dat steeds meer criminele organisaties zich zullen richten op de sociale netwerksites.[66] Dit is letterlijk gebeurd door Britse gevangenen die zich via naar binnen gesmokkelde telefoons manifesteerden op Facebook met dreigementen aan het adres van hun slachtoffers.[67]

2.7.3 Consumentenautoriteit

Wat betreft het misbruik van sociale netwerksites heeft de Consumentenautoriteit (CA) in Nederland aangegeven meer aandacht te gaan besteden aan sociale netwerksites als Hyves en Facebook. Volgens een woordvoerder krijgt deze organisatie steeds meer signalen dat daar praktijken plaatsvinden die niet helemaal in de haak zijn:

> ''De netwerksites zijn grote kanalen aan het worden waar steeds meer commerciële partijen zich op richten. Wij willen weten wat daar gebeurt'', aldus de woordvoerster. Volgens de CA maken commerciële aanbieders dankbaar gebruik van de profielen op die sites om mensen gericht te benaderen en weten mensen die benaderd worden, vaak niet dat er een commerciële partij achter zit.''[68]

De Consumentenautoriteit kijkt ook naar onder andere datingsites die resultaten beloven die niet worden waargemaakt:

> ''Daar wordt vaak iets beloofd wat mensen vervolgens niet krijgen'', 'En daar worden grote bedragen voor neergeteld.'' Zo worden mensen die op zoek zijn naar een partner gekoppeld aan mensen waarvan het profiel helemaal niet overeenkomt. ''Of er komt geen match tot stand, alhoewel dat wel beloofd wordt.''[69]

De vraag is of de aanbieder een inspannings- of resultaatsverplichting heeft. Doorgaans zal niet meer dan bemiddeling worden aangeboden, zoals bij vacature- en dating-sites. Voor de Consu-

[66] http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threatpredict_1209_v2.pdf, MacAfee, threat report 2010.

[67] De netwerksite Facebook heeft op last van de Britse justitie dertig pagina's van gevangenen op Facebook verwijderd. De gevangenen hadden de pagina's aangemaakt via gesmokkelde mobiele telefoons. Op de pagina's werden slachtoffers of hun familie uitgescholden en bedreigd. http://nos.nl/artikel/135996-gevangenen-bedreigen-slachtoffers-via-facebook.html

[68] Consumentenwaakhond wil aan de slag op netwerksites, *Volkskrant* 28 januari 2010.

[69] *Volkskrant* 28 januari 2010 (zie noot 68)

mentenautoriteit zal het niet eenvoudig zijn hard te maken dat hier sprake is van misleiding of mogelijk zelfs oplichting, hoewel de open norm van de "oneerlijke handelspraktijk" wellicht nog wel een aardige stok biedt om deze aanbieders te slaan.

3 Enkele andere Web 2.0 toepassingen

De in het vorige hoofdstuk behandelde sociale netwerksites zijn de voornaamste exponent van Web 2.0 en worden daar soms ook mee vereenzelvigd. In dit hoofdstuk worden kort een groot aantal andere toepassingen toegelicht, waarvan verschillende geïntegreerd kunnen worden in de door de gebruikers van sociale netwerksites beheerde profielen. We streven niet naar een uitputtende inventarisatie, maar behandelen belangrijke of in het oog springende toepassingen.

3.1 File sharing, P2P

Filesharing is het delen van bestanden via het internet met derden. In de regel gaat dit om muziekbestanden, films of software. Een van de populairste manieren van filesharing is het zogenaamde peer-to-peer (P2P) systeem, populaire programma's zoals Emule, KaZaa, Azureus en Bittorrent maken gebruik hiervan.

Filesharing is nog steeds een juridisch probleemgebied. Downloaden van muziek en films mag, mits dat uitsluitend voor eigen gebruik, op beperkte schaal en zonder commercieel oogmerk gebeurt. Het verspreiden van auteursrechtelijk beschermde werken is illegaal. Hierin schuilt een probleem: de meeste file sharing programma's bieden namelijk automatisch bestanden aan nadat deze zijn gedownload. Bij sommige toepassingen wordt zelfs nog tijdens het downloaden dat deel van een bestand wat gedownload is aangeboden aan anderen. Downloaden gaat op deze manier vaak hand in hand met verspreiden. Bovendien worden niet per se volledige bestanden verspreid. Een illegale film kan afkomstig zijn van verschillende bronnen en hoe is achteraf te bewijzen welke bron voor welke maat en welk deel verantwoordelijk is voor het geschonden auteursrecht?

Op filesharingsites als 4Shared of Rapidshare worden bestanden wel in z'n geheel aangeboden. Hier kan men dus downloaden van een illegale bron. Dat voornoemde sites wellicht in beginsel opgezet zijn om het makkelijker te maken voor mensen om onderling

bestanden uit te wisselen (bijvoorbeeld vakantiefoto's) wil niet zeggen dat er geen auteursrechtelijk beschermd materiaal wordt aangeboden. Dit argument werd al gebruikt in de Amerikaanse rechtspraak bij de eerste P2P-dienst, Napster,[70] en later ook in de KaZaa-zaak. Bij alle P2P-systemen wordt vermoedelijk het leeuwendeel van de uit te wisselen bestanden in strijd met het auteursrecht aangeboden.

In Nederland bestrijdt onder andere de Stichting Bescherming Rechten Entertainment Industrie Nederland (Brein) illegale verspreiding van auteursrechtelijk beschermde werken, recentelijk ondermeer in de al eerder genoemde rechtszaken tegen The Pirate Bay alsmede tegen Mininova.[71]

3.2 Films en foto's delen

Bij sites met foto- en videobestanden gaat het primair om rechten van anderen (auteursrecht, privacy), hoewel ook hier vergelijkbare inmengingen in de persoonlijke levenssfeer van de uploader spelen. Foto en video "community sites" combineren e-mail en andere dienstverlening met uitwisseling van persoonsgegevens zoals ImageShack (fotosharing), Heavy.com en uiteraard YouTube (videosharing) en Flickr (fotosharing).

Gmail nodigt uit om toch vooral je foto's op te slaan op de Google server waarbij je vervolgens nog nadrukkelijker wordt uitgenodigd om die foto's te delen met anderen. Hier worden weer allerlei advertenties op gebaseerd die ook met de gmail kunnen worden verzonden of gewoon op je (gedeelde) fotosite verschijnen, natuurlijk gebaseerd op het geselecteerde profiel van de gebruiker. Zoals Google stelt in een zogenaamde privacy mededeling:

> "Net als andere webdiensten slaat Google informatie op over activiteiten die via het desbetreffende account plaatsvinden (bijv. hoeveel geheugenruimte u gebruikt, hoe vaak u inlogt), getoonde of aangeklikte gegevens (zoals UI-elementen, advertenties, links), en andere log-informatie (zoals browsertype, IP-adres, toegangsdatum en -tijd, cookie-ID en doorverwijzings-URL)."

[70] Zie ook paragraaf 5.3
[71] Rb. Utrecht 26 augustus 2009, LJN BJ6008.

Veel gebruikers nemen dergelijke overdadige registratie van informatie voor lief in ruil voor de geleverde dienst onder het mom van "voor wat, hoort wat."

3.2.1 Youtube

Als op Youtube een zelfgemaakt filmpje wordt geplaatst, bijvoorbeeld een opname van jezelf als je een instrument bespeelt of zingt, is dit filmpje in beginsel niet aan auteursrecht onderworpen anders dan dat je zelf het auteursrecht daarop hebt. Dit is alleen anders wanneer bijvoorbeeld werk van een bekende artiest wordt gecoverd. Echter, de muziekclips dan wel tv-series (weliswaar veelal in 'parts' opgedeeld) maken een groot deel uit van wat er op Youtube wordt aangeboden en dit is in beginsel auteursrechtelijk beschermd materiaal. Zoals in het inleidende hoofdstuk aangegeven wordt ook in Nederland opgetreden als auteursrechten via Youtube worden geschonden.

In Amerika is Google inmiddels gesommeerd om alle gegevens over via Youtube bekeken videoclips te overhandigen aan het entertainmentbedrijf Viacom, dat Youtube beschuldigt van auteursrechtenschending.[72] Ook indien iemand een filmpje heeft gemaakt waar per ongeluk iemand op staat die hier geen toestemming voor heeft gegeven, kan op grond van het portretrecht bezwaar worden gemaakt. In juli 2008 is er uitspraak gedaan in de zaak Viacom/Google:[73]

> US District Court Judge Louis Stanton backed Viacom's request for data on which YouTube users watch which videos on the website in order to support its case in a billion-dollar copyright lawsuit against Google.

3.2.2 Youtubisering strafrecht

Harm Brouwer van het OM waarschuwde begin februari 2008 voor wat hij noemde de Youtubisering van het strafrecht. Hij doelde daarmee niet op initiatieven zoals de nagespeelde overval die in december 2007 door het korps Rotterdam-Rijnmond op Youtube werd geplaatst, maar foto's van winkeldieven of filmpjes van criminele activiteiten door burgers, al dan niet op heterdaad 'gevan-

[72] *Viacom sues Google over YouTube clips*, 13 maart 2007, http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html

[73] http://afp.google.com/article/ALeqM5hty1hXgakr7zoviTVNKalsStgSOw

gen'.[74] Ook hier kunnen digitale sporen een klein vergrijp lang kenbaar houden, maar ook anderszins is de vraag of dergelijke enthousiaste burgermanszin niet meer kwaad dan goed doet. Het zal niet de eerste keer zijn dat een vermeende pedofiel gelyncht wordt en naderhand voor een ander blijkt te zijn aangezien. Burgers gaan wat onvoorzichtig om met het beginsel presumptio innocentia. Zo onderging ene Johan van der Sloot uit Drachten in 2008 nog de pijnlijke gevolgen voor Joran (van der Sloot) te worden aangezien. Nu Van der Sloot in mei 2010 een volgende moord bekend heeft, loopt deze Johan dit gevaar mogelijk opnieuw.

Het past niet in het Nederlands strafrecht dat na een veroordeling de daaraan ten grond liggende misstap de veroordeelde nog (lange tijd) nagedragen wordt, althans dit geldt voor de meeste misdrijven. De idee is dat als men zijn straf heeft uitgezeten met een schone lei begonnen wordt. Het plaatsen van films waarop tot in lengte der dagen te zien is hoe een winkeldief een diefstal pleegt, zal dit uitgangspunt in het Nederlandse strafrecht geen goed doen.

3.2.3 Dumpert.nl

Vrij extreem is de onder de paraplu van Geenstijl opererende Dumpert.nl, waar foto's, films en audio kunnen worden "gedumpt". Het lijkt of deze site geen gebruiksvoorwaarden of privacy reglement kent, althans zelfs na herhaaldelijk rondbrowsen op de site hebben we deze niet kunnen vinden. Er zijn echter indringende beeldverslagen te vinden. Medio 2008 bijvoorbeeld een meisje dat huilend haar vader mobiel belde dat ze zo stom was geweest (ze had geblowd) en een aantal keer bijna haar telefoon onder kotste. Niet direct de momenten waar je op een later tijdstip nog eens mee geconfronteerd wil worden door bijvoorbeeld je toekomstige baas. Of neem het filmpje van 16 februari 2008 getiteld "Gekke man gaat los in Metro calandlijn" dat gaat over "Zit je gewoon rustig in de metro gaat er opeens iemand los op zijn hardcore." Of je hiertegen succesvol kan optreden is de vraag (zie uitgebreid hoofdstuk 9). De uiteraard ludiek bedoelde voorwaarden van moederbedrijf Geenstijl zijn weinig hoopgevend:[75]

[74] Zie over dit onderwerp H.H. de Vries, Het spanningsveld tussen privacybescherming en criminaliteitsbestrijding. Zwarte lijsten in de praktijk, in A.R. Lodder & A. Oskamp (red.), *Caught in the Cyber Crime Act*, Kluwer 2009.
[75] http://www.geenstijl.nl/paginas/huisregels.php

> "De huisregels kunnen op ieder moment naar goeddunken van de Redactie ter plekke aangepast worden. Beroepen op de regels is derhalve zinloos, wij hebben altijd gelijk."

Toch wist in september 2009 een studente met succes af te dwingen dat een weinig flatteus filmpje van haar in dronken toestand op de openbare weg werd verwijderd. Het beroep van Geenstijl op de nieuwswaarde van de film ("laten zien hoe ernstig het met dronkenschap onder studenten is gesteld") mocht niet baten.[76]

3.3 Bloggen

Een al wat langer bestaande Web 2.0 toepassing is het zogenaamde weblog.[77] Een weblog is een website waarop korte berichten geplaatst worden, zogenaamde blogs. Hoe accuraat en vaak de weblog wordt bijgehouden is afhankelijk van de blogger, ofwel auteur van de weblog. Een weblog is wellicht het best te omschrijven als een logboek met bepaalde informatie. Deze informatie kan door anderen, bezoekers van de weblog, bekeken worden en vaak kunnen deze bezoekers een reactie op de weblog plaatsen. Er zijn talloze soorten weblogs. Bekende voorbeelden zijn de weblogs met foto's (fotoblog), video (vlog) of audio (podcast), maar ook een lifelog (soort online dagboek), babysite (weblog waarop ouders hun oneindige stroom aan foto's en teksten over hun baby kwijt kunnen) en nieuwslog (online krant waar vaak zeer recent nieuws op te vinden is) zijn bekende vormen.

3.3.1 IT en Recht blogs

Op het gebied van IT en recht zijn er verschillende blog-sites. De site recht.nl is op vrijwel alle rechtsgebieden actief, waaronder Recht en Technologie, en verzamelt actuele informatie maar plaatst geen blog-berichten.[78] De waarschijnlijk oudste IT recht blog is de wekelijks ook rondgemailde Weblog van het advocatenkantoor SOLV.[79] De meest bezochte en zeker die met het grootste aantal reacties is de blog van Arnoud Engelfriet.[80] Er zijn ook blogs die mogelijk wel gelezen worden, zeker interessante informatie

[76] http://blog.iusmentis.com/2009/09/28/geenstijl-moet-privacyschendend-majesteit-filmpje-verwijderen-van-dumpert/, zie over deze zaak ook paragraaf 9.2.1.
[77] Voor een overzicht van de juridische aspecten van bloggen, zie http://www.iusmentis.com/maatschappij/juridisch/bloggen/
[78] http://www.recht.nl/nieuws/ict/
[79] http://www.solv.nl/weblog/
[80] http://blog.iusmentis.com/

bevatten, maar waar bijzonder weinig gereageerd wordt, zoals *Future of copyright* (Bart Schermer e.a.) en *Jurel* (Arno Lodder e.a.).[81] Deze sites zijn wel opgezet als blog-sites, maar missen een belangrijk element, namelijk interactie met de gebruiker. Dit geldt overigens evenzeer voor de blog van SOLV.

3.3.2 Blook – dagboekvaneenkindermeisje.com

Een interessant fenomeen is de zogenaamde blook, een weblog in boekvorm.[82] In 2007 verscheen het boek Dagboekvaneenkindermeisje.com van "Nadine S.", wat een pseudoniem van de Nederlandse schrijfster Karin Overmars bleek te zijn. Het boek was een weergave van de door Overmars aangemaakte thread op het forum Fok!. Zowel de posts van Overmars zelf als de reacties van gebruikers werden (integraal) in het boek weergegeven. Op Fok! ontstond na publicatie van het boek ophef over de vraag wie het auteursrecht bezat op de forumposts van de gebruikers en of Overmars deze wel zonder toestemming in haar boek mocht opnemen.[83]

3.4 Twitter

Een speciale, bijzonder populaire vorm van bloggen is het zogenaamde micro-bloggen, bekend van met name de site Twitter.com. Op Twitter kunnen alleen berichten worden geplaatst met een maximum lengte van 140 tekens, niet toevallig identiek aan de omvang van een SMS-bericht. Behalve via het internet kunnen berichten ook via SMS-berichten naar een Twitter-account worden gestuurd.

[81] http://futureofcopyright.com en http://jurel.nl.

[82] Een van de eerste blooks was *User Interface Design for Programmers* van Joel Spolsky. Binnen Internetrecht is Lawrence Lessig *Code: And Other Laws of Cyberspace, Version 2.0* een mooi voorbeeld: "This second edition, or Version 2.0, has been prepared through the author's wiki, a web site that allows readers to edit the text, making this the first reader-edited revision of a popular book." Zie http://codev2.cc/

[83] http://frontpage.fok.nl/nieuws/207380/1/1/50/ophef-over-boek-van-het-fok-forum.html

Op 22 november 2009 werd het woord Twitter door het genootschap Onze Taal[84] tot woord van het jaar uitgeroepen. Kort na deze kwalitatieve beoordeling, werd ook op kwantitatieve gronden (meest gebruikte woord in 2009) de populariteit van Twitter bevestigd:[85]

> Global Language Monitor's vast survey of print and social media places Twitter ahead of Obama and H1N1 as most used word

3.4.1 Voorwaarden

Een reden waarom mensen Twitter gebruiken is om geïnteresseerden op de hoogte te houden van waar je bent, wat je meemaakt, etc. De aanbieder van de dienst Twitter gaat niet over de inhoud, laat staan dat zij enige aansprakelijkheid aanvaardt:

> You are responsible for your use of the Services, for any content you post to the Services, and for any consequences thereof. (...) Under no circumstances will Twitter be liable in any way for any Content

Als auteur van de zogenaamde tweets houdt je de auteursrechten op de tweets, maar verleent tevens een bijzonder exclusieve licentie aan Twitter:

> You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)

Wat betreft het verdere (commerciële) gebruik door Twitter is niet helemaal duidelijk of zij bedoelt de materialen te willen aanpassen voor verspreiding, slechts ten behoeve van de gebruiker of ook voor andere (commerciële) doeleinden:

[84] http://nos.nl/artikel/98937-twitteren-woord-van-het-jaar-2009.html
[85] http://www.guardian.co.uk/books/2009/nov/30/twitter-declared-top-word-of-2009

> 'You agree that this license includes the right for Twitter to make such Content available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use.'

Bovenstaande bepaling zou kunnen betekenen dat aanpassing noodzakelijk is om de Tweets over verschillende media te verspreiden, maar lijkt tevens opening te bieden aan commercieel gebruik van het materiaal door Twitter. De eventueel daarmee gegenereerde inkomsten worden uiteraard niet uitgekeerd:

> 'Such additional uses by Twitter, or other companies, organizations or individuals who partner with Twitter, may be made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services.'

3.4.2 Zeven redenen van Schermer

Deze voorwaarden weerhouden, uiteraard, mensen niet om Twitter te gebruiken. Bart Schermer noemt maar liefst 7 redenen waarom je Twitter zou moeten gebruiken:[86]

1. Twitter is voor moderne kenniswerkers cruciaal om op de hoogte te blijven van de laatste trends en ontwikkelingen in hun vakgebied en helpt hen om nieuwe leads en business te genereren;
2. Belangrijke mensen (...) twitteren;
3. Met Twitter blijf je altijd op de hoogte van het allerlaatste nieuws;
4. Twitter is een democratiserend medium. Twitter was bijvoorbeeld voor de Iranese oppositie zo'n beetje de enige manier om te communiceren en informatie over de opstand naar buiten te brengen. Twitter stelde zelfs het onderhoud aan haar servers uit om de Iranese oppositie niet af te sluiten van de buitenwereld;
5. Twitter is de volgende Google. (...) Twitter wil binnen vijf jaar één miljard gebruikers hebben en 1,5 miljard euro omzet genereren;
6. Als jurist moet je begrijpen hoe Twitter werkt om je cliënten goed te kunnen adviseren;

[86] B. Schermer, 'Twitter jij al?', *Tijdschrift voor internetrecht* 2009/4.

7. Twitter roept allerlei interessante juridische vragen op.

Niettegenstaande deze fraaie opsomming realiseert Schermer zich terdege dat een belangrijke beweegreden is dat mensen vooral graag 'kwetteren' over zichzelf en daar anderen in willen laten delen.

3.4.3 Kamerdebatten

In de politiek wordt uitgebreid van Twitter gebruik gemaakt. Rijkswaterstaat gebruikt een Twitter account (@rijkswaterstaat) om de hinder van werkzaamheden te beperken. Ook in de Kamerdebatten wordt regelmatig aan Twitter gerefereerd. In april 2009 zijn de eerste opmerkingen over Twitter in de Handelingen te vinden. Op 23 april 2009 vond de volgende uitwisseling plaats.

> De voorzitter: Ik hoor een telefoon. Dat kan niet waar zijn.
> Mevrouw Blanksma-van den Heuvel (CDA): Niet van mij. Twitter?
> De voorzitter: Er wordt hier niet getwitterd of gebeld.
> Mevrouw Verdonk (Verdonk): Twitteren is zo leuk. Ik kan het de voorzitter aanraden.
> De voorzitter: Maar niet tijdens het debat. We gaan door.

Een dag later werd de voorzitter wederom met Twitter geconfronteerd:

> (…) het enige dat de heer Boekestijn in de lucht houdt is twitter
> De voorzitter: Daar zijn er wel meer van.[87]

Sindsdien wordt er druk getwitterd en komt Twitter ook regelmatig ter sprake tijdens de vergaderingen in de Kamer. Zo gaf tijdens de bespreking van de wet kinderombudsman in april 2010 de heer Dibi (GroenLinks) aan:[88]

> Mevrouw Dezentjé is ook actief op Twitter. Ik las daar dat zij de kinderombudsman zelfs beschreef als een nieuw links loket, op kosten van de belastingbetaler.

[87] *Kamerstukken* II 2009-2010, 26 488, nr. 181, Behoeftestelling vervanging F-16, VERSLAG VAN EEN ALGEMEEN OVERLEG.
[88] Handelingen TK 2009-2010, 79

Bij de bespreking in mei 2010, tenslotte, inzake de noodplannen voor de Euro[89] zei Irrgang (SP):

> De minister noemde het op Twitter een antispeculatiemechanisme.

Waarop minister de Jager reageerde met:

> Het stond wel tussen quotes!

Het mag duidelijk zijn dat Twitter een vaste plaats in de politiek heeft verworven. Los van de hierboven al aangestipte aansprakelijkheid en auteursrechten spelen bij Twitter nog diverse andere juridische aspecten, zoals privacy. Het voert te ver om op deze plaats hier uitgebreid op in te gaan.[90]

3.5 Sociale Web 2.0

Sociale Web 2.0 klinkt als een pleonasme, maar wordt hier gebruikt om drie toepassingen te bespreken waar het sociale aspect zo mogelijk nog meer op de voorgrond treedt. Achtereenvolgens wordt ingegaan op social commerce, social bookmarking en calenders 2.0.

3.5.1 Social commerce

Social commerce is vrij vertaald sociale handel. Gebruikers bieden zelf hun producten aan of verwijzen naar sites waar een bepaald product het goedkoopst is. Gebruikers kunnen dus onderling informatie uitwisselen betreffende welk product het goedkoopst is en waar het te vinden is. Social commerce strekt zich uit tot allerlei soorten producten.

Er zijn ook sites waar je aanbevelingen krijgt voor muziek die het beste bij je past (Pandora).

---

[89] Handelingen TK 2009-2010, 82

[90] Zie *More on Legal Issues Related to Twitter and Other Social Media*, http://legalblogwatch.typepad.com/legal_blog_watch/2009/05/more-on-legal-issues-related-to-twitter-and-other-social-media.html and *TWITTER - NEW OPPORTUNITIES AND HEADACHES FOR COMPANIES*, http://howardriceconnect.com/ve/ZZbUJ75M61tM28UV/VT=0/page=3 en Wilson, C. L. (2010) Twit or tweet? legal issues associated with Twitter and other microblogging sites. In, *GikII 2009*, Amsterdam, the Netherlands 17 - 18 Sep 2009.

PANDORA

Dit wordt met behulp van zogenaamde recommender systems[91] afgeleid uit je opgegeven muzikale voorkeuren. Regelmatig zal op deze wijze zeer goed bij de gebruiker aansluitende, maar voor hem onbekende muziek worden aangeraden. De site van Pandora is om auteursrechtelijke redenen medio 2010 alleen vanuit Amerika bereikbaar:[92]

> Dear Pandora Visitor,
>
> We are deeply, deeply sorry to say that due to licensing constraints, we can no longer allow access to Pandora for listeners located outside of the U.S. We will continue to work diligently to realize the vision of a truly global Pandora, but for the time being we are required to restrict its use. We are very sad to have to do this, but there is no other alternative.
>
> We believe that you are in Netherlands (…)

Je hebt ook sites waar je zelf je laatste koopjes kan plaatsen, zodat andere gebruikers op ideeën kunnen worden gebracht, zoals bij productvergelijkings-site Kelkoo.[93]

kelkoo

Je zoekt producten, vergelijkt ze op specifieke kenmerken en prijs, leest de recensies van anderen, maakt je keuze en klikt door naar een koopsite. Web 2.0 heeft er voor gezorgd dat deelnemers een

[91] Ook wel recommendation systems of recommendation engines genoemd. De term recommender systems werd in 1997 voorgesteld door Resnick en Varian, die stelden dat deze een manier waren om aanbevelingen van mensen te verzamelen en door te spelen naar andere mensen, aldus R. Sie, De kracht van recommender systems, *De connectie* 2007/4, p. 10-11.
http://www.deconnectie.com/docs/vorige_connecties/pdfs_van_artikelen/c09-verbeter-de-wereld-met-AI/10-11.pdf
[92] http://www.pandora.com/restricted
[93] http://www.kelkoo.nl/

stap verder kunnen gaan. Ze kunnen namelijk zelf producten vergelijken en aanbevelen aan andere deelnemers via sites als Kaboodle en Tagworld.[94]

3.5.2 Social bookmarking

Hoewel sinds de opkomst van de zoekmachine Google gebruikers steeds slordiger worden in het systematisch beheren van regelmatig bezochte websites, kunnen favoriete sites nog steeds via de in iedere browser aanwezige functionaliteit 'bookmarken' worden opgeslagen. Links naar je favoriete sites kun je ook delen met anderen. Midden jaren negentig gebeurde dit doorgaans door een lijstje links op je homepage op te nemen, onder de noemer ´favorite links´, waarbij ook wel geordend werd naar type sites (personen, hobby, specialisaties, etc.). Deze lijstjes werden allemaal handmatig aangemaakt en in de html-code geknipt en geplakt. Tegenwoordig zijn hier speciale programma's voor met een veel grotere, interactieve functionaliteit.

De toepassing wordt social bookmarking genoemd. Ben je fan van Madonna? Kijk wie welke fansite van Madonna in zijn bookmark heeft. Wil je meer weten over onroerend goed? Kijk welke makelaar website het meest is bezocht. Dit is een alternatieve manier om informatie in het web te vinden, die door en voor Web 2.0 deelnemers tot stand is gekomen. Traditionele zoekmachines zoals Google gebruiken algoritmes met behulp waarvan niet altijd de gewenste informatie gevonden wordt. Bij Google telt wat de meerderheid wil en vindt zwaar mee. Via de door social bookmarking geboden dienst kun je laten meewegen wie bepaalde informatie aanraadt en kan ook minder populaire informatie gevonden worden.

[94] http://www.kaboodle.com/ en http://www.tagworld.com/

Er zijn verschillende social bookmarking tools die je op je web-browser of op een website kan installeren. Een voorbeeld van een social bookmarkingtool is Addthis.[95]

> AddThis helps website publishers and bloggers spread their content across the web by making it easy for visitors to bookmark and share content to their favorite social destinations. AddThis is fast, powerful and easy to install. Even better, it's free and offers sophisticated analytics to help users understand how and where their content is being shared.

Als je een website hebt met informatie kan je een addthis-tool installeren, zodat bezoekers informatie van jouw website kunnen toevoegen aan hun facebook-account, furl-account of andere al dan niet op Web 2.0 gebaseerde sites. Ze kunnen middels die tool ook informatie van jouw website naar andere mensen mailen. Sommige online kranten zoals BN/DeStem hebben zelf social bookmarkknopjes om het nieuws, of althans een deel daarvan, middels een bookmarktool te verspreiden. Ook in Podcasts van radio-uitzendingen kan soms tot op de seconde nauwkeurig worden aangegeven wanneer de stream moet starten, daarbij geholpen door hiervoor door de aanbieder ter beschikking gestelde links.

Indien sites het ondersteunen dat de geplaatste informatie verspreid kan worden middels social bookmarking, waarschuwen ze veelal de auteur of uploader van de informatie vooraf dat ze gebruik maken van social bookmarkingtools. Wanneer dan de informatie geplaatst wordt op zo'n site dan geeft hij/zij daarmee impliciet toestemming voor het verspreiden van zijn of haar werk. Als er geen toestemming is gegeven en vooraf niet gemeld is dat bookmarkingstools gebruikt worden, dan ligt het minder duidelijk. Indien slechts een deel van een tekst wordt overgenomen middels een bookmarkingtool, dan valt het onder het citaatrecht (art 15a Auteurswet). Dit kwam ook aan de orde in de zaak Cossmozz vs. Vermeule/BN/DeStem, waarover Engelfriet in zijn blog opmerkt:[96]

[95] http://www.addthis.com/about
[96] http://www.iusmentis.com

> "Met die knopjes voor 'social bookmarking'-links moedigt BN/De Stem haar lezers aan om het artikel op allerlei manieren elders te promoten. De content komt zo op sites als NUjij, eKudos en het Amerikaanse del.icio.us. Als de site zelf mensen aanmoedigt de tekst door te prikken via allerlei media, en er nergens een auteursrechtvoorbehoud staat, dan kun je moeilijk nog volhouden dat die tekst exclusief is en je veel schade lijdt door een herpublicatie."

Het delen van informatie staat centraal bij Web 2.0 en social bookmarking stelt internetgebruikers in staat op een interactieve manier hun kennis te delen.

3.5.3 Calenders 2.0

Van oudsher heeft een agenda een persoonlijk karakter. Op de lagere en middelbare school heeft iedereen de agenda die goed aansluit bij zijn voorkeuren. De buitenkant was bedoeld voor iedereen, de binnenkant in beginsel alleen voor de gebruiker. Het internet ondersteunt het delen van inhoud, dus de afspraken in de agenda. Een digitale agenda kan beschikbaar worden gemaakt voor vrienden en familie. Ook kun je mensen schrijfrechten geven. Stel dat je bijna jarig bent en wil dat niemand het vergeet, dan kun je vermits je schrijfrechten hebt, dan kun je in de agenda's van je vrienden vermelden dat je binnenkort jarig bent. Dit laatste is ook te realiseren via bijvoorbeeld de events-functionaliteit in Skype.

> "(…) I logged into Skype that morning in the hotel, and when I did an alert popped up. It appeared to be the birthday of our mutual friend and colleague, Colin Rule. So during the Viva I started with asking him whether he had congratulated Colin. This was obviously not the type of question he expected, but I explained the question was not referring to benefiting from Colin's groundbreaking work in Online Dispute Resolution (as we all do), but because it was Colin's birthday."[97]

Bovendien kan iedereen zien wanneer je afspraken hebt of om andere redenen niet beschikbaar bent. Zo kunnen je (virtuele)

[97] A.R. Lodder, Preface bij de handelsuitgave van het proefschrift uit 2008 van Pablo Cortés (2010), *Online Dispute Resolution for Consumers in the European Union*, Series: Routledge Research in Information Technology and E-Commerce Law.

vrienden zien wanneer je het te druk hebt en wanneer je tijd hebt om afspraken te maken. Voorbeelden van Web 2.0 calenders zijn:

- www.rememberthemilk.com;

- www.rsscalendar.com en;

- en www.hipcal.com.

Minder direct, maar voor het plannen van een gezamenlijke afspraak veel gebruikt zijn sites als datumprikker.nl

Afhankelijk van de afgegeven machtigingen kan de Outlook-agenda vergelijkbare functionaliteit leveren. Hiermee vergelijkbaar is Google Agenda. Voordeel van deze toepassing is dat de agenda via het internet door meerdere gebruikers te bekijken is. Google Agenda kan ook prima gebruikt worden om afspraken gerichter te plannen, te meer daar deze vrijwel continu kan worden

bijgewerkt, zie bijvoorbeeld onderstaande mededeling bij een Google Agenda:[98]

> This is the full gory detail of my calendar, mirrored in near real-time.
> Orange means "abroad". Click on the boxes for more details on where.
> If you want to send me a "when can you make it" email, please check here first for empty slots.

3.6 Chat sites

Chatsites creëren een sociale omgeving waarin mensen via het internet 1-op-1, 1-op-n of n-op-n kunnen communiceren met behulp van tekst, beeld en geluid. De eenvoudigste manier om te chatten is via een tekstveld over en weer korte tekstuele berichten uitwisselen. MSN is een van oudsher bekende aanbieder van chatdiensten (hoewel geen webdienst). Waar in het verleden een onderscheid bestond tussen het uitwisselen van tekstberichten, geluidsberichten en videoberichten, is tegenwoordig een combinatie van deze drie vormen mogelijk. Zo is Skype de bekendste internettelefoon aanbieder (chat via video), maar ondersteunt ook het uitwisselen van enkel tekstberichten. Aan de andere kant ondersteunt MSN inmiddels ook geluid- en beeldcommunicatie.

Het is de bedoeling dat chatsites een veilige omgeving leveren. Naast openbare chatsites zijn er ook andere manieren van chatten via internet. Tegenwoordig kan je via sociale netwerksites, zoals Hyves, ook chatten. Op de meeste chatsites bestaat er tijdens het 'chatten' de mogelijkheid om documenten en videobeelden naar elkaar te versturen. Hierdoor is de mogelijkheid gecreëerd om ook kinderpornografisch materiaal naar elkaar te versturen via chatsites.

3.6.1 Minderjarigen en seksuele handelingen

Door personen met een voorliefde voor kinderporno, of anderszins in jeugdigen geïnteresseerden, wordt ook wel tijdens het chatten geprobeerd om minderjarigen over te halen om seksuele handelingen te verrichten. Dit kan dan vervolgens worden vastgelegd met behulp van de webcam waarmee men elkaar kan zien. Een

[98] http://www.cs.vu.nl/~frankh/diary.html

hierbij gebruikte methode is om in eerste instantie betrekkelijk onschuldige foto's met slechts gedeeltelijk ontblote lichaamsdelen te maken met behulp van een webcam. Deze foto's worden vervolgens gebruikt om de gefotografeerde onder druk te zetten en te dwingen om letterlijk meer bloot te geven. Dit roept vragen op over wie verantwoordelijk en aansprakelijk zijn.[99]

De rechtbank Breda oordeelde in 2004 over een poging om via chatcontacten seksueel contact te krijgen met een minderjarig meisje.[100] Tijdens het chatten heeft de verdachte (waarschijnlijk met behulp van een webcam) pornografische foto's van het meisje genomen en deze vervolgens via het internet verspreid. De verdachte is veroordeeld tot een gevangenisstraf van 18 maanden. Het opvallende echter is dat de aansprakelijkheid alleen bij de verspreider wordt gelegd. In een zaak voor de Rechtbank Zutphen uit 2006 ging het om afpersing en vrijheidsberoving, nadat iemand via een chatsite naar een plaats was gelokt door de verdachte.[101]

3.6.2 Veilig internetten voor kinderen

Een aantal chatsite beheerders hebben afgesproken de chatomgeving zo veilig mogelijk voor kinderen te maken. Hiervoor zijn door de projectgroep 'Veilig internetten voor kinderen' Richtlijnen opgesteld.[102]

In het kort houden deze richtlijnen in dat je nooit persoonlijke gegevens (adres, telefoonnummer, etc.) moet geven, niet zomaar een foto moet plaatsen, dat je een goed wachtwoord moet hebben en voorzichtig moet zijn met het gebruiken van de webcam. Een extra waarborg die de richtlijnen bieden is dat elk chatsite een helpknop moet hebben voor eventuele klachten en dat er een toezichthouder (moderater) is die de gesprekken in de gaten houdt.

[99] Rechtbank Haarlem van 24 december 2004 (LJN AR8212).
[100] Rechtbank Breda 29 april 2004 (LJN A08758).
[101] Rechtbank Zutphen 30 augustus 2006 (LJN AY7194).
[102] Zie www.chatinfo.nl

3.6.3 Grooming

Sinds 1 januari 2010 is ook het zogeheten 'grooming' strafbaar gesteld. Artikel 248e Sr bepaalt:

> Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst een persoon van wie hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van zestien jaren nog niet heeft bereikt, een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met die persoon te plegen of een afbeelding van een seksuele gedraging waarbij die persoon is betrokken, te vervaardigen wordt, indien hij enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.

Een begrijpelijke ontwikkeling, maar vanuit strafrechtelijk perspectief bezien niet onomstreden. Al langere tijd kent het strafrecht niet alleen de strafbaarheid van de poging tot een misdrijf maar ook de strafbare voorbereidingshandelingen. De voorwaarden waar bij die laatste groep aan voldaan moet worden strekken ver (zoals georganiseerd verband, strafmaximum tenminste 8 jaar, etc.). In het nieuwe artikel 248^{e} Sr kan voldaan zijn aan "enige handeling gericht op het verwezenlijken" zonder dat de dader daadwerkelijk het oogmerk heeft om de minderjarige te ontmoeten. De bewijslast wordt hiermee omgedraaid. Er wordt aangenomen dat het oogmerk op het daadwerkelijk verwezenlijken van de ontmoeting aanwezig is, en het is aan de verdachte om het tegendeel te bewijzen. Gezien de kwetsbaarheid van de slachtoffers is het te rechtvaardigen dat de bewijslast op de verdachte rust.

3.7 Wiki sites

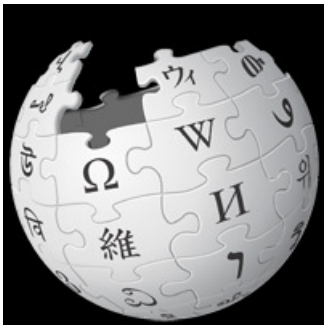
Wikisites zijn internetsites die gebruik maken van de wikitechniek. Wiki is een techniek om gezamenlijk de inhoud van een website te maken. Een opvallend kenmerk van een wiki is dat niemand de baas is over de informatie. De informatie kan door iedereen aangepast en aangevuld worden. Dit kan aan de ene kant waardevol zijn, omdat velen doorgaans meer weten dan één. Aan de andere kant kan het tot een consensus leiden die misschien niet direct gewenst is. Ook is het mogelijk dat een kat-en-muis-spel ontstaat

tussen twee of meerdere personen met tegenovergestelde visies, die de door de anderen geplaatste informatie structureel aanpassen.

Wiki's worden binnen bedrijven, vriendengroepen en universiteiten gebruikt om bijvoorbeeld samen te werken aan een project. De oorsprong van het voorliggende boek is een Wiki-site, namelijk www.internetrecht20.nl. Een andere toepassing is het communiceren van de gebruikte protocollen in een bedrijf naar de medewerkers toe. Een verandering in een protocol is dan ook snel bij iedereen bekend.

3.7.1 Wikipedia

De verreweg bekendste Wiki-site is Wikipedia, een online encyclopedie die wordt samengesteld door de gebruikers zelf.[103]



De naam Wikipedia is een samenvoeging van Wiki en Encyclopedia. De doelstelling van Wikipedia is om in elke grote taal een complete, rechtenvrije encyclopedie op het internet te creëren. Wikipedia wil alle kennis die mensen hebben verzamelen en samenvatten. Pagina's en artikelen van Wikipedia kunnen door internetgebruikers van de site worden aangemaakt, aangepast en bewerkt. Deze aanpak moet ervoor zorgen dat onjuiste informatie snel wordt gevonden en verbeterd.

[103] Een prachtige internet governance analyse van deze site is te vinden in J. ZIttrain, *The future of Internet* (Chapter 6 The Lessons of Wikipedia), Yale University Press, p. 2008, p. 127-148.

3.7.2 Wikipedia als rechtsbron

In 2008 bepaalde een Amerikaans gerechtshof dat Wikipedia niet voor juridische doeleinden mag worden gebruikt. Daarvoor bevat Wikipedia een "verontrustend aantal voorbehouden ten aanzien van de juistheid van informatie".[104] In deze zaak bepaalde de rechter:[105]

> We know only that the BIA thinks that if, hypothetically, the IJ had not considered Wikipedia and reached the same conclusion, then that conclusion would not be clearly erroneous. But we do not know whether the IJ would have reached the same conclusion without Wikipedia, or whether (and, if so, why) the BIA believes that the IJ's consideration of Wikipedia was harmless error, in the sense that it did not influence the IJ's decision. Because the BIA's ultimate conclusion that Badasa failed to establish her identity is not adequately explained, we must remand for further proceedings.

In Nederland blijken rechters incidenteel Wikipedia te raadplegen, zo constateerde Maurice Schellekens.[106] In zijn conclusie van juni 2006 onderbouwde advocaat-generaal Machielse de stelling "De slaap is een bekende kwetsbare plek in de schedel." met een verwijzing naar Wikipedia's lemma Slaap (anatomie).[107] In een arrest van de Hoge Raad van 5 juni 2007 werden definities voor speed en amfetamine aan Wikipedia ontleend.[108] En in een merkenzaak werd zelfs de verwatering van een merk mede beoordeeld aan de hand van informatie over de merknaam in Wikipedia![109]

Maar er zijn ook zaken waarin Wikipedia de rechtszaal niet binnenkomt. Zo mocht van de Vreemdelingenrechter Wikipedia niet gebruikt worden als bron:[110]

> Voornoemde bron kan naar het oordeel van de rechtbank, zonder nadere motivering van verweerder, niet als betrouwbare bron worden aangemerkt. Informatie van internet is niet zonder meer betrouwbaar en/of volledig zonder

[104] *Rechter mag niet op Wikipedia vertrouwen*, Nu.nl 3 september 2008, http://www.nu.nl/internet/1728206/rechter-mag-niet-op-wikipedia-vertrouwen.html
[105] http://www.wired.com/images_blogs/threatlevel/files/badasa.pdf
[106] http://vortex.uvt.nl/TILTblog/?p=42
[107] Hoge Raad 19 september 2006, LJN AX 9404.
[108] Hoge Raad 5 juni 2007, LJN AZ8803.
[109] Vzr. 's-Gravenhage 29 april 2008, LJN BG3086.
[110] Rechtbank 's-Gravenhage, zittingsplaats Amsterdam, 29 juni 2006, LJN AZ2550.

na te gaan wie die informatie heeft geplaatst en of derden deze informatie kunnen wijzigen.

Drion betoogt dat rechters die menen te moeten googelen dan wel in de Wikipedia spieken, dit altijd eerst aan partijen voor moeten leggen voordat zij dit betrekken in hun oordeel. Artikel 149 lid 2 Rv biedt volgens hem geen grond om informatie van internet als feiten van algemene bekendheid aan te merken.[111] De gemiddelde rechter moet echter wel in staat worden geacht om een juiste inschatting te maken over de juistheid van op internet beschikbare informatie.

3.8 Online geschillenoplossing 2.0

Online geschillenoplossing biedt de mogelijkheid om problemen rondom Web 2.0 toepassingen op te lossen. Hoe dienen geschillen binnen Marktplaats of Youtube opgelost te worden? Daar Web 2.0 gebaseerd is op interactiviteit van gebruikers ligt het voor de hand de gebruikers in eerste instantie zelf te laten zoeken naar een oplossing. Online geschillenoplossing biedt vaker een goedkopere en snellere oplossing dan reguliere rechtspraak.[112] Online geschillenoplossing kan relatief eenvoudig zijn. Zo heeft eBay een lijst van voorkomende problemen en mogelijke suggesties om deze problemen op te lossen. Hiermee worden gelijk al een groot aantal conflicten opgelost.

Web 2.0 toepassingen leiden zoals iedere sociale interactie tot nieuwe conflicten. Men kan denken aan negatieve reacties op Hyves over een persoon of over problemen rond de levering van spullen via Marktplaats. Niet echt het type conflict waarbij de rechter meteen wordt ingeschakeld. Vaak zijn de belangen klein en de kosten (zowel tijd/financieel/emotioneel) van reguliere rechtspraak niet in verhouding tot het probleem. Online geschillenoplossing kan bijdragen aan het oplossen van dit soort conflicten. Hierbij kan behalve aan bestaande toepassingen[113] ook gedacht worden ook aan geschillenoplossingsdiensten waarin de Web 2.0 filosofie centraal staat. Hierover schreef Marta Poblet:[114]

[111] http://njblog.nl/2009/03/30/de-onderzoekende-enof-googelende-rechter/
[112] A.R. Lodder & J. Zeleznikow (2010), *Enhanced dispute resolution through the use of information technology*, Cambridge University Press.
[113] In Nederland bijvoorbeeld JURIPAX en e-court.nl.
[114] M. Poblet, 'Introduction: Bringing a New Vision to Online Dispute Resolution', *Proceedings of the 5th International Workshop on Online Dispute Resolution*, in con-

> "(…) a new ODR paradigm in which the center will be neither the online component nor the disputes to be resolved, but the individual people, communities, organizations, and institutions that have to deal with disputes and conflicts and will use the Web to manage and get them resolved in a more effective, efficient, and inexpensive way. This will bring to a new vision on how disputes may be managed and resolved in the information society. This is a vision that not only transforms the field of ODR, but also the very essence of justice and law by making them more horizontal. In sum, a paradigm of relational justice and law"

3.9 Application Programming Interface

Een Application Programming Interface of API is een technologie waarmee functionaliteit van een website of dienst geautomatiseerd kan worden aangeroepen. Door de API kunnen externe partijen gebruik maken van een dienst en kan functionaliteit worden toegevoegd aan een eigen dienst of website.

3.9.1 Mashup

Via de Google Maps API kan een interactieve kaart worden toegevoegd aan een bedrijfswebsite, waarmee bezoekers de route naar een vestiging van het bedrijf kunnen plannen. Zo'n combinatie staat bekend als een mashup.

Bij een mashup worden verschillende informatiebronnen en diensten gecombineerd tot een nieuwe dienst. Zo kunnen recensies van restaurants worden gecombineerd met een kaartdienst zoals Google Maps en de informatie van 9292ov.nl om snel een route naar een restaurant met goed eten te kunnen vinden.

Programmeurs die een API willen gebruiken, moeten vaak een gebruiksrechtovereenkomst (End-User License Agreement of EULA) sluiten voordat ze toegang krijgen. In deze EULA staat dan dat de gebruiker de data slechts voor bepaalde doelen mag gebruiken,

junction with the 21st International Conference on Legal Knowledge and Information Systems (JURIX 2008), Firenze, Italy, December 13, 2008.

op door de site voorgeschreven manieren tonen en geen misbruik van de dienst mag maken.

Steeds meer diensten eisen daarbij dat een programmeur een API key, een unieke code, aanvraagt om een mashup te kunnen bouwen met hun dienst. De mashup moet dan deze code meesturen bij elk verzoek om informatie. Die code is op zichzelf niet beschermd. Wel krijg je de API key pas nadat je akkoord bent gegaan met de EULA waarin staat dat het verboden is de API key aan anderen ter beschikking te stellen. Publiceer je hem toch, dan schend je dus de EULA. De dienst mag je dan afsluiten.

3.9.2 Hyves API

Sites bieden vaak zelf een API aan. Zo kan met de Hyves API toegang gekregen worden tot informatie van profielen. In de privacy policy van Hyves staat:

> "Verder is het zo dat Hyves derden de mogelijkheid geeft om applicaties te ontwikkelen op basis van de Hyves API,te ontwikkelen. Dit zijn, kort gezegd, applicaties die gebruik maken van Hyves. Deze applicaties worden gemaakt door derde partijen die niet aan Hyves gelieerd zijn. Ze worden dus niet door, voor of namens Hyves gemaakt. Hyves heeft geen invloed op de werking van deze applicaties of wat er met de verstrekte gegevens gebeurt als je gebruik maakt van een dergelijke applicatie. Als je een applicatie toestemming geeft voor het gebruik van jouw (persoons)gegevens, valt dit dan ook buiten de verantwoordelijkheid van Hyves. Je kunt je verstrekte toestemming altijd zelf weer intrekken."

Hyves vrijwaart zich dus voor aansprakelijkheid voor privacyschendingen door derden. De Hyves API is een omgeving waarbinnen veel verschillende programma's kunnen worden bedacht, ontwikkeld en gebruikt. Hyves heeft zelf geen directe invloed of zeggenschap over wat er precies wordt ontwikkeld en gedaan. Dit zou Hyves wel kunnen krijgen door zelf bepaalde maatregelen te nemen. Er kan bijvoorbeeld gedacht worden aan een vereiste certificatie voor applicaties. Aan deze certificatie kunnen dan door Hyves bepaalde (privacy)eisen worden gesteld. Op dit moment lijkt het er echter op dit geen prioriteit is.

Ontwikkelaars krijgen echter slechts toegang tot de profielinformatie, foto's, vriendenlijsten en anonieme informatie die al zicht-

baar zijn voor reguliere Hyves-gebruikers. Om deze gegevens vervolgens te gebruiken moet de gebruiker inloggen op de applicatie met zijn Hyves profielgegevens. De externe applicatie krijgt zo toegang tot een profiel. Gebruikers realiseren zich dikwijls niet wat dit voor privacyconsequenties heeft of kan hebben.

3.9.3 Scrapen

Behalve dat sites zelf veelal een API aanbieden, kan de gewenste functionaliteit ook verkregen worden door het zogenaamde scrapen. Hoewel scrapen technisch minder betrouwbaar is, heeft het als voordeel dat je de EULA die vaak bij de API verplicht gesteld is, kunt omzeilen. Een juridisch risico bij scrapen is dat dit een schending van een databankrecht kan opleveren.

4 Virtuele werelden

In de meest brede zin wordt met de virtuele wereld wel gerefereerd aan alles wat zich afspeelt op het internet, van e-overheid tot elektronische handel. Hierbij wordt dan een onderscheid gemaakt tussen enerzijds de fysieke wereld en anderzijds de online wereld. In het verleden ontstond bij aanvang van werkgroepen of bijeenkomsten over virtuele werelden[115] veelal discussie over wat nu precies tot het onderwerp virtuele wereld diende te worden gerekend. "Alles wat zich online afspeelt" is te breed als object van nader onderzoek. Uiteindelijk gaat het in dergelijke discussie voornamelijk om de vraag of sociale netwerksites nu wel of niet tot de virtuele wereld moeten worden gerekend.

4.1 Driedimensionale simulatieomgevingen

Tegenwoordig wordt de term virtuele wereld vrijwel uitsluitend gebruikt voor driedimensionale via internet aangeboden simulatieomgevingen, en vallen daarmee sociale netwerken dus niet onder virtuele werelden. Hoewel er duidelijke verschillen zijn, blijft het onderscheid enigszins kunstmatig: binnen virtuele werelden vinden bijvoorbeeld allerlei activiteiten plaats die vergelijkbaar zijn met het doel waarvoor sociale netwerksites worden gebruikt.

In de op dit moment gebruikelijke omschrijving is een virtuele wereld een computersimulatie van een omgeving die kan variëren van een enkel huis tot een stad of complete wereld of zelfs alternatief universum. De interactie tussen spelers in een virtuele wereld vindt plaats via hun avatar, een driedimensionale grafische weergave van een doorgaans op een mens of dier gelijkende entiteit, ook wel spelkarakter genoemd. Virtuele werelden worden aangeboden in de vorm van een spel (zoals World of Warcraft) maar ook 'lossere' virtuele werelden zoals het vooral bij de jeugd populaire Habbo Hotel of Second Life zijn mogelijk. Een tussenvorm is bijvoorbeeld de Grand Theft Auto serie, waarin de speler

[115] Zoals bij de eerste bijeenkomst van de NVvIR studiecommissie virtuele werelden in 2006, de werkgroep van ECP.NL over gaming en een expert meeting virtuele werelden georganiseerd door Rathenau en XS4all in Nemo in 2007.

een crimineel in een fictieve stad speelt. Hij kan door de spelleiding uitgezette opdrachten proberen uit te voeren, of zijn eigen weg gaan, of een combinatie daarvan.

Net als de hierboven gememoreerde discussies over de reikwijdte van het begrip virtuele wereld, zal op voorhand niet direct voor iedereen helder zijn dat virtuele werelden in engere – en inmiddels 'ingeburgerde' – zin onderdeel uitmaken van Web 2.0. De reden is dat bij virtuele werelden de door een producent aangeboden wereld voor een deel vormgegeven wordt door de spelers. Naarmate het karakter van de wereld meer open is, is het Web 2.0 gehalte groter. Echter ook in die virtuele werelden waar de door producent aan de deelnemers geboden ruimte voor eigen initiatief beperkt is, is de interactie en communicatie binnen de wereld het resultaat van de input van de spelers. In die zin vervagen bij virtuele werelden ook duidelijk de grenzen tussen consument en producent.[116] Hetgeen zich binnen het spel afspeelt is immers anders dan bij offline games voor een groot deel afhankelijk van de input van de deelnemers.

Het recht rond virtuele werelden wordt afzonderlijk bestudeerd en beschreven,[117] reden waarom hier volstaan wordt met een beknopte uiteenzetting over de juridische status van virtuele werelden, voorafgegaan door een introductie in de twee belangrijkste exponenten van virtuele werelden. Om te beginnen het online spel World of Warcraft en daarna de virtuele wereld waar Web 2.0 meest prominent is, namelijk Second Life.

4.2 World of Warcraft

World of Warcraft (WoW) is de grootste en succesvolste virtuele wereld. WoW is een zogeheten MMORPG dat staat voor 'Massively multiplayer online role-playing game'.

[116] Zie ook paragraaf 1.3.
[117] A.R. Lodder (2006)(red.), *Recht in een virtuele wereld: Juridische aspecten van Massive Multiplayer Online Role Playing Games (MMORPG)*, nr. 23 van de NVvIR Publicatiereeks, NVvIR studiecommissie Virtual Law, Elsevier juridisch 2006, Jacob van Kokswijk & Arno R. Lodder (2008), *Recht in Online Reality. De juridische werkelijkheid in fantasiewerelden*, Uitgeverij Paris, B.T. Duranske (2008), *Virtual Law: Navigating the Legal Landscape of Virtual Worlds* (American Bar Association, 2008) en G. Lastowska, *Law and virtual worlds*, te verschijnen (2010/11).

Het spel wordt in abonnementsvorm aangeboden door Blizzard Entertainment. De wereld speelt zich af in een Tolkien-achtige fantasiewereld, waar dwergen, gnomen, trollen en diverse andere personages alomtegenwoordig zijn. Spelers kunnen queestes proberen te vervullen - alleen of in een groep - of zich op andere manieren vermaken, bijvoorbeeld als leerlooier in een dorp. Het universum van WoW is in principe onbeperkt in omvang. Periodiek voegt Blizzard uitbreidingen toe aan de gebieden, personages en mogelijkheden.

WoW begon in 2003. Sindsdien is het spel wereldwijd razend populair geworden, met name in Azië. Er is ook een bloeiende economie rondom deze virtuele wereld ontstaan. Zo is het mogelijk om spelobjecten te kopen en verkopen voor echt geld via veilingsites als eBay of Marktplaats, ondanks het feit dat de spelregels dit verbieden. Het is zelfs mogelijk om een compleet personage te laten ontwikkelen op bestelling. In een lage lonenland, zoals China, wordt dan gespeeld met dit personage om het tot het gewenste niveau van capaciteiten te brengen. Dit is een al langer bestaand fenomeen dat bekend staat als gold farming, ook wel aangeduid als digitale sweatshops.

In de Nederlandse documentaire Cyberkoelies uit 2006 bleek dat in een van de locale Chinese gold farming bedrijven de Chinese World of Warcraft gamers met 10 uur spelen minder dan 2 dollar

verdienen.[118] Een westerse speler betaalt bij een van de vele aanbieders op internet bijvoorbeeld 139 dollar voor een karakter dat van 1-60 gespeeld wordt en 228 dollar voor level 1-70. Zelfs als hier een uur of 50 voor nodig zou zijn, is de winst bijzonder groot. Lucratieve business dus. De spelvoorwaarden verbieden dit zogenaamde goldfarming, maar optreden zeggen de spelaanbieders lastig te vinden.

4.3 Second Life

Second Life is een virtuele wereld opgezet door het Amerikaanse bedrijf Linden Lab.

In tegenstelling tot spelgeoriënteerde virtuele werelden zoals World of Warcraft heeft Second Life geen inherent doel. Een ieder is vrij om de wereld te verkennen en te doen wat hij wil, of dat nu kletsen met vrienden is, ontdekkingstochten uitvoeren, of het verkopen van digitale t-shirts aan andere avatars.

De economie van Second Life is gebaseerd op de Linden Dollar, een virtuele geldeenheid die naar echt geld om te zetten is. Het bedrijf verkoopt land en Linden Dollars. Spelers kunnen onderling elk object maken dat zij willen, en deze aan elkaar verkopen, ruilen of schenken. Second Life draait op user-generated content en is daarmee een prominent voorbeeld van een virtuele wereld die onder de noemer Web 2.0 kan worden geschaard.

[118] http://jurel.nl/2007/08/04/no-more-cyberkoelies/

Linden Lab is uniek in haar benadering dat spelers eigenaar zijn van hun virtueel bezit. Veel andere virtuele werelden eigenen zichzelf juist alle rechten op in-game objecten toe. Virtueel geld (omdat dit in echt geld kan worden omgezet) en voorwerpen worden om deze reden een interessant object voor diefstal en andere vormen van criminaliteit.

Linden Lab sluit in haar Terms of Service aansprakelijkheid uit op de meest uiteenlopende gebieden en behoudt zich daarnaast het recht voor om actie te ondernemen tegen ongewenst gedrag. Eén van de sancties is bijvoorbeeld het opheffen van het account.

Second Life werpt juridische vragen op inzake eigendomsrecht en auteursrecht. Welke rechten hebben auteurs en makers als kopiëren van een object werkelijk gratis en onbeperkt mogelijk is? Moet Second Life een kunstmatig octrooi- of auteursrechtensysteem invoeren en afdwingen? Momenteel stellen de Terms of Service van Second Life dat auteursrecht binnen Second Life gevestigd kan worden indien dit in een toepasbare wet voorzien is. Deze omschrijving laat veel ruimte voor discussie open. Bovendien blijkt uit de Terms of Service dat niet alleen de auteur maar ook Linden Lab vergaande (aan het auteursrecht verwante) rechten verwerft zodra inhoud wordt gecreëerd.

4.3.1 Virtuele kinderporno

Second Life raakte in februari 2007 in opspraak wegens virtuele kinderporno. Virtuele kinderporno, waarbij de afgebeelde kinderen niet daadwerkelijk zijn misbruikt, is sinds 1 oktober 2002 strafbaar.[119] Het zou hierbij moeten gaan om beelden die levensecht zijn. De vraag is in hoeverre er in Second Life sprake is van "niet van echt te onderscheiden" beelden. Het in de Nederlandse wetgeving en jurisprudentie aangelegde criterium is overigens strenger dan "realistisch" uit het Cybercrime verdrag, waar de virtuele kinderporno bepaling op gebaseerd is. Beelden in Second Life zul-

[119] Kamerstukken II 2001–2002, 27 745

len vooralsnog wel duidelijk van echt te onderscheiden blijven, maar kunnen desalniettemin realistisch zijn, zeker wanneer als maatgevend de beleving van kinderen wordt genomen.

4.3.2 Virtuele diefstal

In New York is in oktober 2007 de eerste rechtszaak ingediend over diefstal in Second Life.[120] De verdachte, zo wordt althans gesteld, bezocht virtuele winkels en kopieerde daar onder meer speelgoed en kleding. Deze objecten werden vervolgens verkocht.

> Linda Eros claims that Thomas Simon stole specific computer code to copy products she created and sells in the virtual Second Life world.

Voor het Nederlands recht is het interessant dat de man de spullen kopieerde. Artikel 310 Sr vereist namelijk dat het goed wordt weggenomen. In het geval van de diefstal in New York zou er naar Nederlands strafrecht geen diefstal hebben plaatsgevonden, omdat na de kopieerhandeling het object ook nog steeds in het bezit van de oorspronkelijke eigenaar is.

In het Nederlandse recht zijn er inmiddels verschillende uitspraken over virtuele diefstal, waarbij nadrukkelijk is bepaald dat kopiëren geen diefstal oplevert, maar dat het wegnemen van virtuele objecten als diefstal kan worden gekwalificeerd.[121]

4.4 Juridische status virtuele werelden

De juridische status van virtuele werelden biedt veel stof voor discussie. Virtuele werelden worden gereguleerd met een gebruiksovereenkomst. Daarmee is vrijwel alles contractueel dichtgespijkerd, wat de beheerders een disproportionele grote macht geeft tegenover de gebruikers. Is dat wenselijk?

Sommige virtuele werelden zijn binnen een bepaalde 'tijd' en/of plaats gesitueerd. Zo speelt World of Warcraft zich in een Tolkien-

[120] http://www.tgdaily.com/business-and-law-features/34598-lawsuit-filed-over-virtual-theft-in-second-life

[121] Rb. Leeuwarden 21 oktober 2008 (Runescape), LJN BG0939, Hof Leeuwarden 10 november 2009, LJN BK2773 en Rechtbank Amsterdam 2 april 2009 (Habbo), LJN BH9789, LJN BH9790 en LJN BH9791.

achtige fantasiewereld in een grijs verleden af. Is het daar toelaatbaar dat spelers zich niet over moderne zaken mogen uitlaten (discussies over het werk) of zich mogen profileren op een manier die de beheerders niet vinden passen bij fantasiewerelden (bijvoorbeeld een gay/lesbian avonturiersgroep)?

Sommige virtuele werelden zijn gebaseerd op films of boeken. Zo kunnen spelers zelf een ruimteschip besturen in het Star Trek universum. Dit roept interessante auteursrechten- en merkenvragen op. Mag een speler in dit universum bijvoorbeeld zijn eigen Enterprise bouwen? Of een Millennium Falcon uit het concurrerende Star Wars universum?

Er zijn ook conflicten in de virtuele wereld. Hoe dient men hier mee om te gaan? Veelal zal er slechts een overeenkomst zijn tussen de aanbieder en de spelers, maar niet tussen de spelers onderling. Ook de algemene voorwaarden zijn in beginsel alleen van toepassing op de twee partijen die de overeenkomst hebben gesloten. Een derde die niet betrokken is bij die overeenkomst zou dan moeten eisen dat een andere speler zich moet houden aan de overeenkomst die hij/zij met de gebruiker heeft gesloten. Men zou dan bijvoorbeeld kunnen stellen dat door het niet handelen conform de algemene voorwaarden die de maker van een virtuele wereld gebruikt de wederpartij een onrechtmatige gedraging doet tegenover andere spelers die zich wel houden aan dezelfde bepalingen in hun overeenkomst.

Voorop in het Nederlands recht staat dat overeenkomsten alleen werken tussen partijen. In het Mooijman/Netjes arrest[122] heeft de Hoge Raad bepaald dat indien er sprake is van een feitelijke samenwerking die ervoor zorgt dat een partij alleen zijn werkzaamheden kan uitvoeren indien de andere partij zijn contractuele verplichtingen nakomt, de niet nakoming van de overeenkomst ook onrechtmatig kan zijn tussen de partijen die geen overeenkomst hebben gesloten. Dit zou wellicht van toepassing kunnen zijn als sommige spelers zodanig het spel frustreren dat men het niet meer naar behoren kan spelen.[123]

Tenslotte, het is de vraag of de virtuele wereld wel echt zo wetteloos is als het voor sommigen lijkt. Veelal zijn immers reguliere wettelijke bepalingen van toepassing op de virtuele wereld. Echter

[122] Hoge Raad 29 mei 1998, NJ 1999, 98.
[123] Dit alleen voorzover het Nederlandse recht van toepassing. Dit is veelal niet zo, omdat de aanbieders vanuit andere landen opereren.

de vraag is in hoeverre men dit wil, zeker gezien het spelkarakter van virtuele werelden. Bij virtuele werelden is continu een spanning tussen het reguleren (wat een overheidstaak kan zijn) en het niet reguleren. De wijze waarop een virtuele wereld gereguleerd dient te worden is een vraag waar veel discussie over is en het laatste woord daarover is zeker niet gezegd.[124]

[124] Hierbij wordt wel de term Magische cirkel gebruikt om aan te geven dat er een grens is tussen het spel en de dagelijkse werkelijkheid. A.R. Lodder, Virtuele werelden: toepassing externe regulering na afweging in het licht van de magische cirkel, *Ars Aequi* 2008, p. 513-523.

5 Auteursrecht

Auteursrechten zijn sinds het ontstaan van de boekdrukkunst steeds belangrijker geworden. Daarvoor was het schenden van auteursrecht nauwelijks aan de orde, sterker nog *bestond* auteursrechtschending als zodanig niet. Inbreuk was immers alleen middels het overschrijven van de boeken mogelijk, en daar hadden weinig mensen zin in.

In de loop der eeuwen is veel veranderd. Zo werd de boekdrukkunst geautomatiseerd waardoor het interessanter en makkelijker werd om een boek van een ander uit te geven alsof je het zelf geschreven had. Daarnaast ontstonden er in de 18e eeuw ook kopieermachines waardoor het nog makkelijker werd om (een deel van) de tekst van een ander te gebruiken en daardoor het auteursrecht van die ander te schenden. Om het auteursrecht te kunnen inroepen waren er in die tijd afspraken tussen de drukkers en de koningen van het land. In 1912 ontstond de eerste echte Auteurswet, een uitwerking van de Berner Conventie uit 1886.

Door het internet heeft het auteursrecht en de mate waarin de 'gewone man' er mee te maken heeft een vlucht genomen. Iedereen gebruikt informatie van internet en zeker met de opkomst van Web 2.0 wordt op grote schaal auteursrechtelijk relevante content gemaakt en/of van anderen gebruikt. Over wat nu precies wel en niet toelaatbaar is, bestaat nog steeds discussie.

Voor de deelnemer aan Web 2.0 toepassingen is het goed om zich te realiseren wat de juridische status is van het downloaden en vooral het uploaden van auteursrechtelijk relevante informatie. Op sociale netwerksites worden bijvoorbeeld door de deelnemers auteursrechtelijk beschermde werken uitgewisseld. De vraag is of dit nog kan worden gezien als eigen gebruik in kleine kring als die kring potentieel zo groot is als deelnemers aan de sociale netwerksite. Hier speelt een vergelijkbare discussie als bij „ruchtbaarheid geven" in geval van smaad,[125] namelijk in hoeverre een besloten profiel van een sociale netwerksite ook daadwerkelijk als niet openbaar kan worden beschouwd. De positie van de sociale netwerksite exploitant is hierbij ook aan de orde. De vraag is in

[125] Zie hoofdstuk 7.

hoeverre deze toezicht moet houden alsmede of de aanbieder van de sociale netwerksite een beroep op artikel 6:196c BW kan doen als hij geen zicht heeft op de informatie die zich op de accounts van de deelnemers bevindt?

In dit hoofdstuk worden enkele voor Web 2.0 relevante auteursrechtelijke onderwerpen behandeld, waarbij geenszins volledigheid wordt nagestreefd. In paragraaf 5.1 wordt ingegaan op up- en downloaden. In paragraaf 5.2. op file sharing programma's en in paragraaf 5.3. op Creative Commons licenties. In de slotparagraaf 5.4 wordt de auteursrechtelijke status besproken van de bij Web 2.0 toepassingen veel gebruikte embedded links.

5.1 Uploaden, downloaden

Onder downloaden wordt verstaan het elektronisch opvragen van data die zich op een ander computer(systeem) bevinden en deze data vervolgens op de eigen computer (dan wel ander elektronisch apparaat) al dan niet permanent opslaan. Auteursrechtelijk is het downloaden een verveelvoudigingshandeling en het uploaden zowel een verveelvoudigingshandeling als een openbaarmakingshandeling. Het enkel bekijken of beluisteren van werken via het netwerk wordt niet als downloaden gezien, omdat de onvermijdelijke tijdelijke opslag geen zelfstandige economische waarde bezit (artikel 13a Auteurswet). Ook 'browsen' valt niet onder het auteursrecht.

5.1.1 Thuiskopieregeling

In Nederland valt downloaden (min of meer bij toeval) onder het thuiskopie-regime van artikel 16c Auteurswet, indien de download wordt gemaakt voor eigen oefening, studie of gebruik.[126] Het

[126] *Kamerstukken* II 2002/2003, 28 482, nr. 8, p. 13: "De thuiskopie-regeling verbindt aan het privé-kopiëren de voorwaarde dat een vergoeding wordt betaald. Die vergoeding is verschuldigd ongeacht of er sprake is van een legale of illegale bron en wordt geheven bij de producent of importeur en doorberekend aan de consument. Indien bij de vaststelling van de vergoeding de privé-kopie van een illegale bron niet in aanmerking zou worden genomen, dan zou de gebruiker die illegale werken kopieert in feite goedkoper uit zijn. De wet zou dan een premie zetten op gebruik van illegaal werk. Dat dat niet de bedoeling kan zijn verklaart dat ook de richtlijn niet de beperking stelt dat het moet gaan om een legale bron. Het feit dat een heffing is betaald legitimeert overigens niet dat een kopie daarvan vervolgens in omloop of anderszins in het verkeer wordt gebracht. Dat blijft niet toegestaan. Evenmin is toegestaan een privé-kopie in opdracht van derden te maken of een privé-kopie af te geven."

downloaden van muziek en films is toegestaan, ongeacht of deze legaal aangeboden of verspreid (ge-upload) zijn.[127] Zelfs als een internetgebruiker weet dat een werk illegaal is, mag hij deze legaal downloaden. Voor software geldt deze uitzondering niet (artikel 45n Auteurswet), enkel een recht op het maken van back-ups (reserve kopie) bij legaal aangeschafte software.

Door de komst van Web 2.0-applicaties is het verspreiden van auteursrechtelijk beschermde werken zoals foto's, muziek en film toegenomen. Het downloaden van files via P2P-aanbieders of andere Web 2.0 diensten is niet in strijd met het auteursrecht is, maar uploaden is dit ingevolge artikel 1 Auteurswet wel. Het uplaoden is ingevolge artikel 31 dan wel 32 Auteurswet strafbaar, indien dit zonder toestemming van de auteursrechthebbende gebeurt. In de 'ideale' wereld betekent dit dat er geen aanbod is (uploaden is immers niet toegestaan) en de auteursrechthebbenden dus niet bang hoeven te zijn voor inkomensverlies. Zoals bekend wijst de praktijk anders uit.

5.1.2 Artikel 16c "weer te geven"

Artikel 16c lid 1 Auteurswet is verruimd tot "of weer te geven".[128] Hieronder vallen nu ook geschriften, die voorheen nog de bescherming genoten van artikel 16b lid 2 Auteurswet op grond waarvan 'slechts een klein gedeelte van het werk mag verveelvoudigd worden'. Dit heeft als gevolg dat tijdschriften en e-books in zijn geheel kunnen worden gedownload, ook via het illegale circuit. Is het downloaden van een illegale bron dan alleen een 'morele kwestie' geworden, waar hooguit de wat oudere generatie zich nog in einige mate in kan vinden? De meeste mensen zien immers geen enkel probleem in het downloaden van illegale films of muziekbestanden.

5.1.3 Van kleine kring tot de hele wereld

Waar in het verleden de CD (of zelfs nog het cassettebandje en LP, de langspeelplaat) in de familie/kennissenkring de ronde deed om gekopieerd te worden, geldt nu het internet als 'distributiecen-

[127] *Kamerstukken* II 2002/2003, 28 482, nr. 5, p. 33: "Het ontbreken van de eis dat het origineel legaal moet zijn, kan er dus toe leiden dat van een illegale bron legale privé-kopieën worden gemaakt, voor zover de overige voorwaarden die artikel 16c stelt in acht worden genomen. De beperking inzake privé-kopiëren staat het niet toe dat zo'n kopie wordt afgegeven of wordt openbaar gemaakt. (…) Het heeft mijn voorkeur dat alleen van een legale bron een privé-kopie wordt gemaakt."

[128] *Kamerstukken* 2001-2002, nr. 28 482. De bepaling is inwerking getreden op 1 september 2004.

trum'. Voor wat betreft de CD, het uitlenen daarvan aan iemand is toegestaan en ook dat deze daar vervolgens een (thuis)kopie van maakt. Dit is allemaal nog in lijn met de Auteurswet. Zoals gezegd is het 'aanbieden' op het internet (oftewel uploaden) niet toegestaan. Daarin verschilt de huidige praktijk dan ook met name van het kopiëren van pakweg 20 jaar geleden. Daarnaast is het veel grootschaliger geworden. Het is niet noodzakelijk om iemand, tenminste via-via, te kennen om kopieën te maken. Via het downloaden gemaakte kopieën kunnen afkomstig zijn van volledig onbekenden en zullen dit in de meeste gevallen ook zijn. Sterker nog, door P2P software is het doorgaans niet eens duidelijk van wie er een kopie is gemaakt.

5.2 Filesharingprogramma's P2P

Peer-to-peer programma's (P2P) zorgen ervoor dat grootschalige uitwisseling van bestanden kan plaatsvinden. Het P2P-programma wordt doorgaans van internet gehaald en maakt het mogelijk om bestanden van andere computers die dit programma ook hebben te doorzoeken en de daarop aanwezige bestanden te kopiëren. Terwijl iemand zoekt is het tegelijkertijd voor anderen mogelijk om op zijn computer bestanden te doorzoeken en te kopiëren. Het aanbieden van de bestanden (waardoor andere gebruikers dit bestand kunnen kopiëren) wordt uploaden genoemd. Dat laatste is een handeling die, zoals eerder genoemd, krachtens artikel 1 Auteurswet in Nederland alleen voorbehouden is aan de maker/auteursrechthebbende (althans, indien de toestemming van de auteursrechthebbende ontbreekt).

5.2.1 Toegang verlenen tot bestanden

Hoewel er veelal van uploaden wordt gesproken, ook in dit boek, is bij P2P-programma's eigenlijk geen sprake van het plaatsen (uploaden) van een bestand. Bij de klassieke bestanduitwisseling via bijvoorbeeld FTP werd een bestand naar een server geüpload (put) of vandaar gedownload (get). Bij een P2P-programma worden (delen) van bestanden wel van andere computers gedownload, maar ze worden niet ge-upload. Het enige dat de gebruiker doet is anderen toegang verlenen tot op zijn computer aanwezige bestanden.

De term uploaden wordt veelal wel uitwisselbaar gebruikt met het ter beschikking stellen van informatie. Zo is bijvoorbeeld op de site van BREIN te lezen:[129]

> "(…) want als je daarmee downloadt wordt je automatisch uploader, dat is 'ter verspreiding aanbieden' (…)"

Een andere reden dat de term uploaden bij P2P-diensten wordt gebruikt is vanwege het adagium "downloaden mag, uploaden mag niet." Rond de eeuwwisseling werd deze tweedeling duidelijk verwoord in een editorial van *Computerrecht* van Hugenholtz.[130] In een 'bliksemonderzoek' naar de auteursrechtelijke status van Napster kwam hij tot deze conclusie. Dit editorial was een reactie op een onderzoeksronde van NWO (ITeR) waarin overdreven vaak Napster als onderzoeksobject genoemd werd. Hugenholtz kwam zonder noodzakelijk nader onderzoek tot de conclusie dat downloaden juridisch toelaatbaar is, maar het ter beschikking stellen van bestanden een niet toegestane openbaarmakingshandeling betreft.

5.2.2 Tegelijkertijd aanbieden en downloaden

Aanbieders op sites als 4Shared of Rapidshare maken regelmatig inbreuk op het auteursrecht. Hoewel met name in rechtszaken wel gesteld wordt dat dergelijke sites in beginsel bedoeld zijn om 'eigen' files (te denken valt aan foto's of zelf gemaakte filmpjes) met anderen te delen, is het aanbod van auteursrechtelijk beschermd materiaal in ruime meerderheid aanwezig. In tegenstelling tot de torrentsites waar op het moment dat gedownload wordt de bestanden direct ook ter beschikking worden gesteld aan anderen, kan bij Rapidshare of 4Shared gedownload worden *zonder* tegelijkertijd aanbieden van deze bestanden. In dat laatste geval handelt de downloader dus niet in strijd met de Auteurswet als hij auteursrechtelijk beschermde muziek, film of geschriften download.

5.2.3 KaZaa

P2P-programma's maken het mogelijk om auteursrechtelijk beschermde werken openbaar te maken. Een voor de hand liggende stap om het auteursrecht te beschermen is om de maker van het programma waarmee de Auteurswet kan worden overtreden voor

[129] http://www.anti-piracy.nl/nieuws/artikel.asp?artikelid=29
[130] B. Hugenholtz, 'Napster: een bliksemonderzoek', *Computerrecht* 2000/5, p. 288.

de rechter te dagen. In Nederland is onder ander gedaan in de zaak tegen KaZaa.

In zijn arrest van 19 december 2003 heeft de Hoge Raad beslist dat KaZaa niet verantwoordelijk is voor inbreuken op het auteursrecht.[131] De Hoge Raad neemt het oordeel van het Hof over en concludeert dat het verschaffen van middelen voor openbaarmaking of verveelvoudiging van auteursrechtelijk beschermde werken niet zelf een openbaarmakings- of verveelvoudigingshandeling is. Verder wordt ook vastgesteld dat vele type bestanden met dit programma uitgewisseld kunnen worden. Buma/Stemra stelt dat dit andere gebruik betekenis mist, echter hier wordt aan voorbij gegaan door te concluderen dat dit misschien geldt voor Buma/Stemra, maar niet voor de andere gebruikers.

5.3 Enkele buitenlandse uitspraken

5.3.1 Napster

In Amerika is de eerste en bekendste aanbieder van een P2P-programma, Napster, veroordeeld wegens inbreuk op het auteursrecht.[132]

[131] Hoge Raad 19 december 2003, LJN AN 7253. Advocaat Alberdingk Thijm meldde direct via de SOLV blog dat KaZaa legaal was bevonden door de Hoge Raad, zie http://www.solv.nl/weblog/KaZaa-is-legaal/685. Hugenholtz is kritisch in NRC van 22 december 2003: "De Hoge Raad heeft helemaal niets beslist; BUMA is uitgegleden over een juridische bananenschil.", zie http://www.ivir.nl/publicaties/hugenholtz/nrc-KaZaa.html

[132] United States Court of Appeals for the Ninth Circuit 21 februari 2001 (A&M Records inc., Geffon Records etc. vs. Napster inc.), http://caselaw.lp.findlaw.com/data2/circs/9th/0115998p.pdf

Dit kwam onder andere door het verschil in werking tussen Napster en de directe opvolger KaZaa. Het programma van KaZaa is volledig gedecentraliseerd, terwijl het bij Napster gecentraliseerd was. Bij Napster vond de uitwisseling van de bestanden dus plaats via de centrale server van Napster. Bij KaZaa vond de uitwisseling plaats tussen de gebruikers van het programma. Napster kon in tegenstelling tot KaZaa wel invloed uitoefenen ten aanzien van het gebruik van het programma.

5.3.2 USA: Jammie Thomas

Ook de eerste veroordeling van een individuele downloader vond in Amerika plaats. In oktober 2007 is Jammie Thomas wegens het aanbieden van 24 muzieknummers op internet veroordeeld tot het betalen van 222.000 dollar (9250 dollar per nummer).[133] In september 2008 had Thomas beroep aangetekend, met als argument dat de jury nooit de instructie had mogen krijgen om aanbieden als verspreiden te zien. In Amerika is er een onderscheid tussen het aanbieden van beschermde werken en het verspreiden daarvan. Het aanbieden alleen levert niet direct auteursrechtschending op. In Nederland is het aanbieden niet los te zien van het verspreiden. Het beroep leverde Thomas weinig op, want ze werd in juni 2009 opnieuw veroordeeld maar nu voor 80.000 dollar per nummer, wat bij de 24 nummers neerkomt op 1,92 miljoen dollar.[134] In januari 2010 werd de boete door Michael Davis teruggebracht:[135]

[133] *Volkskrant* 5 oktober 2007, http://www.volkskrant.nl/multimedia/article467408.ece/Illegaal_downloaden_kost_vrouw_220.000_dollar

[134] Single-mother digital pirate Jammie Thomas-Rasset must pay $80,000 per song, *Times Online*, http://technology.timesonline.co.uk/tol/news/tech_and_web/article6534542.ece

[135] http://www.webcitation.org/5n2E7HM3z

> Davis used his power of remittitur today to slash the damage award by 97.2 percent, from $1.92 million down to $54,000—and he suggested that even this lower amount was too high.

Enkele dagen later verwierp Thomas een schikkingsvoorstel van de platenmaatschappijen van 25.000 dollar, wat nog steeds een bijzonder hoog bedrag is (nl. iets meer dan 1000 dollar per nummer).[136]

5.3.3 Spanje: Sharemula

In Spanje heeft het gerechtshof van Madrid een voor P2P sites gunstige uitspraak gedaan. Na een klacht van de Spaanse tegenhanger van Brein tegen Sharemula.com verrichte de politie enkele arrestaties. Sharemula is een site met zogenaamde ed2k-links.[137]

De Spaanse rechter in eerste aanleg oordeelde dat de wet niet was overtreden, omdat de beheerders van de site niet uit winstbejag hadden gehandeld. Het gerechtshof bevestigde in hoger beroep het vonnis. Volgens het Hof kwam het verzamelen van ed2k-links niet neer op een schending van het auteursrecht, ondanks dat de links verwezen naar auteursrechtelijk beschermd materiaal. Of er winst met de P2P site gemaakt werd, was volgens het Hof niet relevant.[138] Tegen deze uitspraak van het Hof is geen verder beroep mogelijk. Dit houdt in dat dergelijke linksites nu in Spanje legaal zijn, ongeacht of ze commerciële doeleinden hebben.

---

[136] Settlement Rejected in 'Shocking' RIAA File Sharing Verdict, *Wired* 27 januari 2010, http://www.wired.com/threatlevel/2010/01/settlement-rejected-in-shocking-riaa-file-sharing-verdict/#ixzz0q0STV38n

[137] Dit zijn geen directe links naar een download, maar een link naar een bestand wat zich op het eDonkey/eMule netwerk bevindt. Zie ook uitleg http://www.digimuziek.nl/edonkey.htm: „KaZaa ingewijden kennen ongetwijfeld de Sig2datlinks. eMule kent ook zo'n systeem, de eD2Klinks. Diverse sites publiceren deze links die met één klik een download via eMule kunnen starten."

[138] Spaanse rechter oordeelt dat linksites legaal zijn, *Tweakers.net*, http://tweakers.net/nieuws/55765/spaanse-rechter-oordeelt-dat-linksites-legaal-zijn.html

5.3.4 Duitsland: Rapidshare

In Duitsland is in september 2008 Rapidshare veroordeeld tot het checken van alle uploads op copyrights.[139]

Hashchecking om eerder verwijderde files te weren is onvoldoende. Inmiddels is Rapidshare door de Duitse rechter veroordeeld om al het materiaal dat wordt geüpload te controleren op copyrightschending. Hashchecking om eerder verwijderde files te weren is onvoldoende. In hoger beroep in mei 2010 is door de Duitse rechter bepaald dat Rapidshare niet verantwoordelijk kan worden gehouden.[140]

5.3.5 Zweden: The Pirate Bay

The Pirate Bay is bij IT juristen in Nederland vooral bekend door de eerder aangehaalde zaken die BREIN tegen ze aangespannen heeft, maar zeker ook vanwege de strafrechtelijke veroordeling in Zweden in 2009.

139 http://torrentfreak.com/rapidshare-to-be-forced-to-shut-down-following-court-defeat-080129/

140 *OLG Düsseldorf: Rapidshare haftet nicht für Urheberrechtsverletzungen*, http://www.heise.de/newsticker/meldung/OLG-Duesseldorf-Rapidshare-haftet-nicht-fuer-Urheberrechtsverletzungen-992144.html

De beheerders van The Pirate Bay werden in deze zaak veroordeeld tot een jaar cel en 2,7 miljoen euro boete.[141] Hierbij moet wel in aanmerking worden genomen dat in de zaak naar voren kwam dat de beheerders van The Pirate Bay aanzienlijke winst boekten met hun onderneming, hoewel zij dit zelf uiteraard tegenspreken.

5.4 Creative Commons

Creative Commons is door Lawrence Lessig opgezet om tegenwicht te bieden tegen de traditionele, gesloten kijk op auteursrechten. Waar auteursrecht als uitgangspunt heeft dat alle rechten voorbehouden zijn en licenties slechts limitatief opgesomde en sterk geclausuleerde toestemmingen verlenen, gaat Creative Commons uit van 'Some Rights Reserved' en licenties die alles toestaan mits aan enkele limitatief opgesomde en sterk geclausuleerde eisen wordt voldaan.

Creative Commons is tot op zekere hoogte te vergelijken met c.q. afgekeken van open source,[142] dat uit midden jaren tachtig stamt. Creative Commons sluit bijzonder goed aan bij Web 2.0. Net als bij open source software is de gedachte dat je in gezamenlijkheid content kan creëren door stukken van anderen te gebruiken. De ervaring leert dat hoewel er op vrij grote schaal content wordt aangeboden onder een Creative Commons licentie, het hergebruik redelijk beperkt is.[143] Het is ook niet zonder gevaar om deze content te gebruiken. De mogelijkheid bestaat immers dat iemand content aanbiedt onder een Creative Commons licentie zonder over het auteursrecht op het aangeboden werk te beschikken. In dat geval loopt de hergebruiker het gevaar aangesproken te worden door de auteursrechthebbende.

Niettemin bieden onder andere de eerder aangeduide prosumenten content aan onder Creative Commons licenties om zo anderen in staat te stellen hierop voort te borduren. Traditionele uitgevers

[141] Zie onder andere 'Court jails Pirate Bay founders', *BBC News*, http://news.bbc.co.uk/2/hi/8003799.stm en *The Pirate Bay Guilty; Jail for File-Sharing Foursome*, http://www.wired.com/threatlevel/2009/04/pirateverdict/

[142] Zie hierover uitgebreid E. Thole, R. Scholten & W. Seinen (red.)(2006), *Open Source Software: Een verkenning naar de juridische aspecten van open source software*, NVvIR studiecommissie, nr. 24 van de NVvIR publicatiereeks, Elsevier-juridisch, www.nvvir.nl/doc/opensourcesoftware.book.pdf

[143] Zie ook kritisch K.J. Koelman (2009), 'Waarom Creative Commons niet kan werken', *Computerrecht* 2009, p. 112.

en informatieverstrekkers hebben hier meer moeite mee, omdat zij het verkopen van (elektronische) exemplaren van werken als enige mogelijke businessmodel zien.

Creative Commons wordt wel gezien als het auteursrecht dat specifiek voor het internet is. Op het internet kan de gesloten-heid/starheid van het auteursrecht een probleem vormen. Indien de maker zijn stukken/werken op internet plaatst om deze zoveel mogelijk te verspreiden teneinde naamsbekendheid te krijgen, biedt het auteursrecht met zijn strakke regime onvoldoende mogelijkheden. Het auteursrecht in Nederland vindt ook zijn oorsprong in de meer traditionele werken waarbij men kan denken aan boeken in gedrukte vorm. Het is dus vanuit de achtergrond van het auteursrecht niet vreemd dat het niet voldoet aan de wensen van makers op het internet.

Binnen Creative Commons worden een drietal zaken relevant geacht voor het beschermen van een werk op het internet:
1. naamsvermelding;
2. commercieel gebruik;
3. afgeleide werken.

Naamsvermelding is cruciaal in de bescherming die de Creative Commons biedt. Men mag het werk gebruiken, maar wel onder vermelding van de naam van de oorspronkelijke maker. Hiermee geeft de maker anderen de mogelijkheid zijn werk te verspreiden op een manier dat de maker naamsbekendheid krijgt.

Een tweede element dat van belang is, is of het werk door derden commercieel gebruikt wordt. Het is niet vreemd dat indien een derde geld verdient aan het werk van de maker, zonder dat de maker daar financieel profijt van ondervindt, de maker dit gebruik kan verbieden.

Tenslotte kan de maker ervoor kiezen dat afgeleide werken niet mogen. Dit houdt in dat men het werk niet mag veranderen. De achtergrond hiervan komt sterk overeen met de persoonlijkheidsrechten in het auteursrecht en het daarin vervatte verbod tot het aantasten van het werk. Indien men dit zou toestaan zou het veranderde werk toegeschreven kunnen worden aan de eerste maker waardoor deze schade zou kunnen leiden. Dit zou bijvoorbeeld een negatieve invloed kunnen hebben op de reputatie van de desbetreffende maker.

5.5 Embedded links

Veel mensen halen materiaal van Youtube af en zetten dit op hun Hyves-profiel of blog. Dit kan door middel van "embedded links". De vraag is of met deze embedded links beschouwd moeten worden als het opnieuw openbaar maken van het achterliggende materiaal zoals een Youtube filmpje.

In 2008 besloot Buma/Stemra om achter bloggers aan te gaan die filmpjes of muziek opnemen in hun blog waar het auteursrecht van berust bij Buma/Stemra. "Embedden is volgens de wet 'opnieuw openbaar maken'", zo zegt Buma/Stemra, en dus is er een webcasting-licentie nodig.

Veel bloggers en mensen die muziek embedden op hun site waren het niet eens met Buma/Stemra omdat zij vinden dat zij niet "openbaar maken" in de zin van de Auteurswet. Zij worden hierin gesteund door jurisprudentie waarin bepaald is dat embedden hetzelfde is als inline linken en linken niet gezien wordt als inbreuk op de Auteurswet.[144]

Na alle commentaren heeft Buma/Stemra vervolgens een nieuw licentiemodel ontwikkeld voor muziek via internet. Hierin wordt een "embedded file licentie" opgenomen. Daarmee kan een muziekverspreider (zoals Youtube) regelen dat anderen filmpjes of muziek mogen embedden op hun site. Youtube en andere muziekverspreiders moeten betalen, maar de embedder wordt gevrijwaard van claims voor gebruik van Buma-repetoire.

Een grote beperking aan die gratis licentie is dat de embedder niet commercieel bezig mag zijn. Een blog of site die geld verdient met de content, moet alsnog betalen, vindt Buma.

Eind 2009 ontstond wederom commotie omtrent embedden. Op 1 oktober 2009 publiceerde Buma haar nieuwe tarieven. Hierin was ondermeer te lezen dat het embedden van 1-6 filmpjes maar liefst 130 euro zou gaan kosten. Na zeer veel protesten werd deze voorgestelde maatregel al weer ingetrokken.[145]

[144] Hof Amsterdam 16 maart 2010, LJN BL7920.
[145] Buma/Stemra slikt embedtarieven in, *Webwereld* 9 oktober 2009, http://webwereld.nl/nieuws/63934/buma-stemra-slikt-embedtarieven-in.html

Zeer opmerkelijk was het arrest van het Hof Den Bosch dat oordeelde op 12 januari 2010 dat embeddden als een openbaarmaking moet worden gezien[146], onder het mom dat dit in de rechtspraak en literatuur betrekkelijk eensgezind wordt aangenomen. Dit is geenszins het geval. Zo had kort voor deze uitspraak Dirk Visser in Mediaforum juist het tegenovergestelde beweerd.[147] Engelfriet constateerde dat de bewuste passage van het Hof zonder verder bronvermelding van de blog van SOLV was overgenomen, saillant genoeg van de advocaat van MyP2P in deze zaak.[148] De discussie hierover is nog niet verstomd.[149]

[146] In de zaak C More Entertainment AB tegen MyP2P Holding B.V.
[147] D. Visser (2010), 'Het 'embedden' van een YouTube-filmpje op een Hyves-pagina', *Mediaforum* 2010/1, p. 12-16.
[148] http://blog.iusmentis.com/2010/01/14/embedden-nu-toch-openbaar-maken/
[149] http://www.solv.nl/weblog/discussie-embedden-kent-geen-einde/16752

6 Aansprakelijkheid

Sociale netwerksites slaan allerhande informatie op van hun gebruikers. In geval deze informatie inbreuk maakt op rechten van anderen, kan de aanbieder van de site in beginsel mede hiervoor aansprakelijk worden gesteld. Als de providers aan de gestelde voorwaarden voldoen kunnen ze zich beroepen op de aansprakelijkheidsuitsluiting van hosting-providers. Deze is op grond van artikel 14 van de Richtlijn 2000/31/EG in het vierde lid van artikel 6:196c BW opgenomen. De aanbieder van de sociale netwerksite is niet aansprakelijk als hij:

> a. niet weet van de activiteit of informatie met een onrechtmatig karakter en, in geval van een schadevergoedingsvordering, niet redelijkerwijs behoort te weten van de activiteit of informatie met een onrechtmatig karakter, dan wel
> b. zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt.

Hosts van sociale netwerksites zoals Hyves, Facebook en LinkedIn zijn niet aansprakelijk voor eventuele onrechtmatige informatie die op hun sites geplaatst wordt, zolang zij hiervan niet op de hoogte zijn en dit ook niet behoren te zijn. Een beheerder van een sociale netwerksite hoeft in beginsel niet te controleren wat door iedereen geplaatst wordt. Dit is ook als zodanig nadrukkelijk bepaald in artikel 15 van de Richtlijn 2000/31/EG, dat er niet een algemene plicht bestaat om informatie te monitoren. Deze bepaling is echter geschreven voor de klassieke internetproviders zoals XS4ALL. Het is de vraag of deze regeling ook onverkort geldt voor sociale netwerksites. Deze kunnen afhankelijk van het doel van de site en welke faciliteiten de site de gebruikers biedt om informatie op te slaan wellicht niet geheel ontkomen aan een plicht om in de gaten te houden welke informatie er op de site geplaatst wordt.

Zodra er een melding binnenkomt over vermeend onrechtmatige informatie dan is het afhankelijk van de aard van de informatie en de hoedanigheid van de melder of de aanbieder van de Web 2.0 dienst genoodzaakt is deze informatie te verwijderen. In redelijkheid moet niet getwijfeld kunnen worden aan de juistheid van de

melding. De praktijk leert dat aanbieders vrij snel geneigd zijn te voldoen aan een verzoek om informatie weg te halen, omdat ze vrezen anders door de melder aansprakelijk te worden gesteld.

In dit hoofdstuk wordt eerst ingegaan op de wijze waarop aanbieders van met name sociale netwerksites trachten hun aansprakelijkheid via algemene voorwaarden uit te sluiten. Hierbij wordt eerst stilgestaan bij de wijze waarop gebruikers aan deze voorwaarden gebonden worden. Daarna zal op een voor aansprakelijkheid van Web 2.0 dienstverleners karakteristieke groep, de forumbeheerders, worden ingegaan. Tenslotte wordt aansprakelijkheid van online veilingsites behandeld.

6.1 Algemene voorwaarden

Aansprakelijkheid op internet is veelal gebaseerd op onrechtmatige daad, maar uiteraard is contractuele aansprakelijkheid (of uitsluiting van aansprakelijkheid via algemene voorwaarden) ook bij Web 2.0 toepassingen relevant.

In veel gevallen is de juridische toelaatbaarheid naar Nederlands recht van de algemene voorwaarden van aanbieders van onder andere sociale netwerksites op zijn minst twijfelachtig. Niet alle aanbieders opereren vanuit Nederland, maar onder gebruikers zitten in alle gevallen ook Nederlandse gebruikers. Het betreft met name bepalingen inzake instemming, dienstverlening en aansprakelijkheid, verantwoordelijkheid voor de inhoud van materiaal, de intellectuele eigendom van materialen, de beschikking over de informatie en de persoonlijke informatie die op de sociale netwerk sites wordt getoond.

6.1.1 Instemming

Om deel te nemen aan een Web 2.0 dienst dienen de gebruikers in te stemmen met de algemene voorwaarden. Zoals gebruikelijk bij de aanbieders van internetproducten en diensten zullen de meeste gebruikers niet veel verder komen dan het zetten van een kruisje in het daartoe bestemde vakje. Desondanks poogt de aanbieder de gebruiker te verleiden tot het zorgvuldig lezen van die voorwaarden. Doet de gebruiker dat dan zijn er nogal wat verrassingen. Doet de gebruiker dat niet, maar maakt hij toch gebruik van

de dienst, dan is hij in ieder geval gebonden. In de voorwaarden van Hyves is bijvoorbeeld te lezen:[150]

> Door gebruik te maken van de website van Hyves – onder meer toegankelijk via Hyves.nl, Hyves.net en Hyves domeinnamen met andere extensies ("Website"), maar ook via andere wegen (bijvoorbeeld via andere (mobiele) media en de Hyves API), op welke manier dan ook, aanvaard je daarmee gebonden te zijn aan deze gebruiksvoorwaarden.

Het enkele gebruik wordt als voldoende grondslag gezien voor binding aan de algemene voorwaarden. Dit is bij een site als Hyves op zichzelf begrijpelijk, omdat degenen die meer kunnen op de site dan alleen kijken, altijd als deelnemer ingeschreven moeten zijn. Tijdens het inschrijfproces kun je dan expliciet worden gewezen op de toepasselijke gebruiksvoorwaarden.

6.1.2 Eenzijdige aanpassing

Vrijwel alle aanbieders vinden het vanzelfsprekend dat zij de voorwaarden eenzijdig kunnen aanpassen en dat de gebruiker zelf, zonder enige kennisgeving, moet zorgen op de hoogte te geraken. Zo stelt, wederom, Hyves:[151]

> Hyves heeft het recht om deze gebruiksvoorwaarden op elk gewenst moment aan te passen, zonder de gebruikers daarvan in kennis te stellen

Dit is een op zichzelf niet ongebruikelijke praktijk, maar zeker bij een online dienst waar de afnemers veelal dagelijks de site bezoeken (de Hyvers) zou het voor de hand liggen om deze wijzigingen te communiceren. Dit kan, zonder dat het de aanbieder veel moeite kost, door duidelijk op een vaste plek op de site een historisch overzicht van de wijzigingen (die toch ook intern zullen worden bijhouden) te geven. Alternatief is om de gebruikers via interne communicatiediensten (zoals mail) desgewenst dagelijks, wekelijks of maandelijks op de hoogte te stellen. Ook dit laatste zal niet erg bewerkelijk zijn voor de aanbieder. Hoewel het bekend is dat gebruikers lang niet allemaal hier in geïnteresseerd zullen zijn en velen nooit van de wijzigingen zullen kennisnemen, wordt zo in

[150] Aanhef van de gebruiksvoorwaarden, http://www.hyves.nl/useragreement/. Facebook kent bijvoorbeeld een identieke bepaling: "By using or accessing Facebook, you agree to this Statement."
[151] Aanhef van de gebruiksvoorwaarden, http://www.hyves.nl/useragreement/

ieder geval de mogelijkheid geboden aan degenen die op de hoogte willen blijven. Het geeft naar deze, en uiteindelijk ook de niet geïnteresseerde groep, een prettiger uitstraling dan de niet bijzonder sympathiek overkomende bepaling hierboven. Een vergelijkbare bepaling is te vinden bij Twitter:[152]

> The Services that Twitter provides are always evolving and the form and nature of the Services that Twitter provides may change from time to time without prior notice to you.

Dit klinkt ingrijpender dan het is. Voor sites die miljoenen gebruikers hebben kan het ondoenlijk lijken om iedereen op de hoogte te stellen van elke wijziging van functionaliteit. Een actieve houding van de gebruikers kan in dezen verlangd worden. Niettemin kan ook in geval van nieuwe of gewijzigde features (de aanbieder zal informatie over alle wijzigingen intern bijhouden), de gebruiker via de hierboven gestelde wijze worden geïnformeerd.

In het verlengde van bovenstaande bepalingen wordt de gebruiker automatisch gebonden geacht aan veranderde voorwaarden, inclusief daar mee gemoeide kosten. Zo stelt MyWeb:

> MyWeb reserves the right to change the terms, conditions, and notices under which it offers the Web Sites, including any charges associated with the use of the Web Sites. You are responsible for regularly reviewing these terms, conditions and notices, and any additional terms posted on any Web Site. Your continued use of the Web Sites after the effective date of such changes constitutes your agreement to them.

Op zich is het niet onredelijk van gebruikers te verlangen dat ze zelf wijzigingen in de gaten houden. Noodzakelijk is dan wel de hierboven gesuggereerde lijst van wijzigingen aan gebruikers ter beschikking te stellen, omdat het ondoenlijk is om zonder deze informatie eenvoudig in de doorgaans uitgebreide voorwaarden eventuele wijzigingen op te sporen. Vooral indien gebruikers niet alleen aan de gewijzigde voorwaarden worden gebonden, maar ook betaling voor, mogelijk aanvullende diensten, verschuldigd zijn. Dit laatste is naar Nederlands recht niet aanvaardbaar. Consumenten mogen niet via gewijzigde algemene voorwaarden zonder enige nadere melding tot betaling van een dienst verplicht

[152] http://www.twitter.com/tos

worden. Ook naar Amerikaans recht is deze handelswijze niet zondermeer aanvaardbaar. Er zullen weinig rechtstelsels zijn waar een consument die zonder kosten van een dienst gebruikt maakt, enkel middels gewijzigde algemene voorwaarden een betalende gebruiker wordt.

6.1.3 Derden

Een opmerkelijke bepaling, tenslotte, is dat je er voor in moet staan dat bepaalde derden zich aan de voorwaarden van Hyves houden:[153]

> (…) dat je er voor instaat dat iemand die van Hyves gebruik maakt op jouw computer zich ook zal houden aan deze gebruiksvoorwaarden.

Deze bepaling is minder vreemd dan hij mogelijk op het eerste gezicht lijkt. Zoals hierboven aangegeven is een gebruiker van Hyves altijd aan de voorwaarden gebonden via de voor het gebruik noodzakelijke registratie. Iemand die een account van een ander gebruikt om Hyves content te bekijken en informatie te plaatsen, is zelf niet aan deze voorwaarden gebonden. Indien er door deze derde handelingen worden verricht in strijd met de gebruiksvoorwaarden moet het voor Hyves mogelijk zijn om iemand daarop aan te spreken. Dit zal dan degene zijn onder wiens naam de gebruiker ingelogd was. Vergelijk het met de bezitter van een auto, waar behoudens tegenbewijs ook vermoed wordt dat de bezitter bestuurder was.

Net als de bestuurder van een auto een minimumleeftijd heeft, is de content op sociale netwerksites en andere Web 2.0 toepassingen niet altijd geschikt voor alle leeftijden. Controle op de leeftijd van gebruikers blijft echter lastig.[154]

6.1.4 Hyves en content

Met uitzondering van Facebook gaan de aanbieders er vanuit dat zij niet verantwoordelijk zijn voor hetgeen binnen hun platform gebeurt. De aanbieders oefenen echter wel degelijk controle uit op de inhoud, presentatie en de diensten die plaatsvinden via hun sociale netwerk. De uitzonderingen van artikel 6:196c BW lijken zeker niet onder alle omstandigheden van toepassing, ongeacht of

[153] http://www.hyves.nl/useragreement/
[154] Zie ook paragraaf 2.5.1.

de aanbieders zich beschouwen als tussenpersonen die 'mere conduit', 'caching', of 'hosting' verrichten. De aanbieders stellen in ieder geval dat zij op geen enkele wijze civiel of strafrechtelijk aansprakelijk kunnen worden gesteld voor hetgeen op hun sociale netwerk plaatsvindt:[155]

> Hyves reguleert de communicatie tussen gebruikers onderling of tussen gebruikers en de dienst van Hyves niet inhoudelijk. Hyves heeft dan ook geen controle over de kwaliteit, veiligheid, rechtmatigheid, integriteit of juistheid van de verschillende onderdelen van de dienst. Hyves is niet aansprakelijk voor handelen of nalaten van haar gebruikers, waaronder begrepen de bestanden, gegevens en/of materialen die zij op de website van Hyves beschikbaar stellen.

Deze uitsluiting is alleen al om die reden niet bijzonder betekenisvol dat hij is overeengekomen in de gebruikersovereenkomst met de Hyver. De partijen bij deze overeenkomst zijn de Hyver en Hyves. Eventuele aansprakelijkheid zal zich uiteraard niet enkel beperken tot geregistreerde gebruikers en bij aansprakelijkheidsstelling van derden kunnen deze niet aan deze bepaling gebonden worden geacht. Tegen de Hyvers zelf is deze bepaling in beginsel wel in te roepen.

Hyves geeft wel aan te bepalen hoe de account wordt ingevuld en behoudt zich het recht voor de account te weigeren en binnen bestaande accounts informatie te modificeren of te verwijderen zonder specifieke toestemming. De grondslag hiervoor is te herleiden tot de aanvaarding van de algemene voorwaarden:[156]

> 5(b) het recht verleent om enige door jou ter beschikking gestelde bestanden, gegevens en/of materialen te verwijderen van de servers van Hyves en van de Website, bedoeld of onbedoeld, en voor welke reden dan ook en ook zonder reden, zonder dat Hyves op welke wijze dan ook aansprakelijk wordt jegens jou of een derde als gevolg van een dergelijke verwijdering.

Hier spreekt een actieve inmenging in de content uit. Daar kan anders dan deze bepaling stelt zeker aansprakelijkheid uit volgen. Stel bijvoorbeeld dat Hyves ten onrechte informatie van een ac-

[155] http://www.hyves.nl/useragreement/
[156] http://www.hyves.nl/useragreement/

count verwijdert waardoor een derde schade lijdt. De hierboven aangehaalde bepaling is niet op deze derde van toepassing. De mogelijkheid bestaat dat Hyves dan met succes aansprakelijk wordt gesteld. In het licht van deze bepaling is het interessant om te vermelden dat Hyves prompt handelt indien een klacht hen bereikt. Ze verleenden bijvoorbeeld medewerking aan notice en vooral takedown van vermeend inbreukmakend materiaal bij de *Peter Pan hoax* van Arnoud Engelfriet en Steven Ras van IC-Trecht.[157] Net als eerder bij het bekende Multatuli voorbeeld van XS4ALL was ook hier het auteursrecht verlopen en derhalve niet sprake van een inbreuk.

6.1.5 Twitter en content

Ook Twitter gaat niet over de inhoud, laat staan dat zij enige aansprakelijkheid aanvaardt:

> You are responsible for your use of the Services, for any content you post to the Services, and for any consequences thereof. (...) Under no circumstances will Twitter be liable in any way for any Content

Op zichzelf een begrijpelijke bepaling, maar zoals hierboven al aangegeven strekken dergelijke voorwaarden zich niet uit tot derden die Twitter aansprakelijk willen stellen. Naast dit leggen van de verantwoordelijkheid voor uitingen bij de gebruiker is de uitsluiting van aansprakelijkheid bij Twitter niet alleen uitputtend in de algemene voorwaarden opgenomen, maar is het de enige bepaling die volledig in hoofdletters is opgesteld:

> TOT HET MAXIMUM DAT DOOR DE WET IS TOEGESTAAN, ZIJN TWITTER EN ZIJN DOCHTERONDERNEMINGEN, GELIEERDE BEDRIJVEN, MANAGERS, MEDEWERKERS, AGENTEN, PARTNERS EN LICENTIEHOUDERS NIET AANSPRAKELIJK VOOR ENIGE DIRECTE, INDIRECTE, INCIDENTELE, CONSEQUENTIE

Een wat merkwaardig einde van de bepaling. Ze zullen aanspraken op schadevergoeding willen uitsluiten. Voor de uitingen zullen ze in beginsel niet aansprakelijk zijn, ze hebben daar geen bemoeienis mee, hoewel ook aansprakelijkheid ook hierbij onder omstandigheden denkbaar is. Voor het niet goed functioneren van de

[157] http://blog.iusmentis.com/2009/04/07/hyves-kletst-in-reactie-op-peter-pan-onderzoek-over-communitysites/

dienst zal, zeker als derden hierdoor schade ondervinden, Twitter aangesproken kunnen worden.

6.1.6 LinkedIn en content

Ook het professionele netwerk LinkedIn trekt zijn handen af van de inhoud en geeft dit voor alle duidelijkheid in hoofdletters aan:

> LINKEDIN AND THE LINKEDIN AFFILIATES ARE NOT RESPONSIBLE FOR A MEMBER'S MISUSE OR MISAPPROPRIATION OF ANY CONTENT OR INFORMATION YOU POST IN ANY FORUMS, BLOGS AND CHAT ROOMS.

Deze bepaling lijkt overbodig, of de strekking komt niet goed over. Waarom zou LinkedIn verantwoordelijk zijn voor misbruik dat anderen maken van informatie dat door de LinkedIn deelnemers is geplaatst? Dat is vergelijkbaar met een krant die haar aansprakelijkheid uitsluit voor wat anderen zullen gaan doen met de informatie van ingezonden brieven. Als een briefschrijver vermeldt dat je bij een bepaalde post beter de belasting kan oplichten, dan is de krant uiteraard niet aansprakelijk voor iemand die vervolgens ook daadwerkelijk de belasting oplicht. Er zijn genoeg andere voorbeelden te verzinnen, maar gevallen waarin aansprakelijkheid zou kunnen volgen voor LinkedIn voor "misuse or misappropriation" van door haar deelnemers geposte informatie zijn niet gemakkelijk te bedenken.

6.1.7 Google Italië

Duidelijk uit de besproken bepalingen is dat aanbieders van Web 2.0 diensten graag aansprakelijkheid uitsluiten. Aan de andere kant willen de aanbieders graag de beschikking houden over de werken, materialen en persoonsgegevens die in de profielen zijn vastgelegd. Dit kan tot juridische problemen leiden. Het is immers het een of het ander: of men wil geen enkele betrokkenheid bij de inhoud of men accepteert die verantwoordelijkheid.

Hoe ver de verantwoordelijkheid kan gaan, ondanks alle prachtige uitsluitingen in de algemene voorwaarden, wordt ondermeer geïllustreerd door twee zaken die eind 2009/begin 2010 speelden in Italie. De eigenaar van YouTube, Google, werd aangesproken op de inhoud van op YouTube geplaatste content. Google diende direct alle video's van het Italiaanse mediaconglomeraat Mediaset, eigendom van Berlusconi, van YouTube te verwijderen. Dat beslis-te een Italiaanse rechter. Mediaset had een rechtszaak tegen

Google aangespannen, omdat er geen toestemming was gegeven voor het plaatsen van 325 uur aan beeldmateriaal van onder meer Big Brother. Google kan ook een schadeclaim van 500 miljoen euro van Mediaset verwachten.

In een andere rechtszaak[158] in Italië is Google (YouTube) verantwoordelijk gesteld voor het uploaden van een filmpje over de mishandeling van een geestelijk gehandicapte jongen. Dit filmpje is in 2006 op YouTube geplaatst. Tegen medewerkers van Google zijn gevangenisstraffen van zes maanden voorwaardelijk uitgesproken. Vreemd genoeg wordt Google, en niet de mensen die het filmpje maakten en uploaden of de mishandelaars, verantwoordelijk gehouden voor de openbaarmaking van de video waarop de mishandeling te zien was. Dit is temeer merkwaardig omdat de video enkele uren na publicatie van YouTube is verwijderd. [159]

De bovenstaande Italiaanse zaken zijn, zeker de laatste, vrij ongewoon. Het illustreert niettemin wat hierboven is aangegeven, dat uitsluiting van aansprakelijkheid enkel geldt voor de afnemer van een Web 2.0 dienst, en niet voor derden die menen schade te ondervinden van op Web 2.0 geplaatste content. Indien rechters zouden doorschieten in het honoreren van claims als met name de laatste, zou dit het einde betekenen van Web 2.0 diensten. Een dergelijk geval deed zich in Nederland voor bij een forumpagina, waarop in de volgende paragraaf uitgebreid wordt ingegaan.

6.2 Forumbeheerders

De rol en verantwoordelijkheid van de forumbeheerder komt in de Nederlandse rechtspraak regelmatig aan de orde. Het gaat daarbij om de vraag in hoeverre de forumbeheerder verantwoordelijk kan worden gehouden voor berichten van de forumgebruiker. De Richtlijn 2000/31/EG inzake de elektronische handel, zoals omgezet in artikel 6:196c BW, regelt zoals bekend de omstandigheden waaronder tussenpersonen op internet *niet* aansprakelijk kunnen worden gesteld voor handelingen van hun gebruikers.

Om de richtlijn te kunnen duiden is het van belang te realiseren dat deze geschreven is in een tijd dat van Web 2.0 nog geen spra-

[158] http://arstechnica.com/tech-policy/news/2009/12/google-defends-itself-in-italian-video-bullying-case.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss
[159] http://weblogs.nrc.nl/media/2009/12/18/google-in-de-problemen-in-italie/

ke was. De rollen waren helder verdeeld indertijd. Er waren providers die toegangsdiensten verleenden (de zogenaamde access-providers), providers die opslagcapaciteit ter beschikking stelden (de zogenaamde hosting-providers) en providers die een noodzakelijke schakel in het verzenden van informatie over internet vormden maar enkel als doorgeefluik (de zogenaamde mere-conduit). In dit rijtje ontbreekt de content-provider, maar die moet, anders dan de hierboven genoemde tussenpersonen, verantwoordelijk kunnen worden gehouden voor de content die deze op het internet plaatst.

In de loop der tijd is de rolverdeling minder duidelijk geworden. Steeds meer providers verlenen verschillende diensten, waarbij ook het onderscheid tussen content providers en de andere drie typen niet altijd meer goed te maken is. Web 2.0 diensten maakt de problematiek nog lastiger. Hierbij staat immers interactiviteit en het aanbieden en delen van informatie door gebruikers centraal. De gebruikers waren in de klassieke situatie enkel afnemer. Het idee was dat de aanbieder als hij geen bemoeienis had met wat er met zijn aangeboden dienst gebeurde (kortweg: geen boodschap aan de boodschap), hij ook niet aansprakelijk kon zijn. Althans, zo lang hij nog niet op de hoogte was gesteld.

6.2.1 Actieve moderator

Inmiddels zijn er verschillende uitspraken over forumbeheerders[160] gewezen. Hierbij doet zich een paradoxale situatie voor. In de klassieke indeling moet de forumbeheerder worden gekwalificeerd als een aanbieder van hosting diensten. De verschillende berichten die de gebruikers posten worden immers opgeslagen door de forumbeheerder. Dit betekent dat als de forumbeheerder zich actief bemoeit met de inhoud, door bijvoorbeeld bepaalde berichten te verwijderen als deze discriminerend of anderszins onrechtmatig dan wel strafwaardig zijn, hij geen beroep kan doen op de uitsluiting van aansprakelijkheid van artikel 6:196c BW. In deze zin is ook geoordeeld door het Europese Hof van Justitie op 23 maart 2010 (Google/Louis Vuitton):[161]

[160] Vzr. Amsterdam 1 november 2007, LJN BB6926 (Martijn), Rb. Amsterdam 16 oktober 2008, LJN BG0972 (Showbiznewz) en Rb. Rotterdam 2 februari 2009, LJN BH1711 (Nationale Alliantie).

[161] *Publicatieblad van de Europese Unie* 22 mei 2010, C 134/2. De uitspraak ging over zoekmachines, maar is in algemene zin van toepassing op dienstverleners van de informatiemaatschappij zoals aanbieders van Web 2.0 diensten.

> (…) wanneer die dienstverlener geen actieve rol heeft gehad waardoor hij kennis heeft van of controle heeft over de opgeslagen gegevens. Indien dat het geval is, kan de dienstverlener niet aansprakelijk worden gesteld (…)

Hiermee is dan nog niet gezegd dat deze beheerder aansprakelijk is, want daarvoor moet worden nagegaan of hij op grond van artikel 6:162 BW aansprakelijk kan worden gesteld. Er is veel voor te zeggen om een actieve moderator het niet aan te rekenen als er toch een bericht doorheen glipt. Zeker van zijn zaak is deze forumbeheerder echter niet. Dit is gek genoeg anders als de forumbeheerder helemaal niks doet. Als hij de grootst mogelijke rotzooi (beledigend, strafwaardig, etc.) op zijn forum toestaat zonder te controleren, kan hij pas aansprakelijk worden als hij op de hoogte raakt hiervan. Aangezien hij het zelf niet in de gaten houdt, is dit alleen na een klacht mogelijk. In dat geval zal hij wel prompt moeten handelen, maar tot die tijd kan alle content er straffeloos staan.

6.2.2 Internetoplichting/Trendylaarzen

Dat de gevolgen ver kunnen strekken bleek bij uitspraken tegen de site *Internetoplichting*, die uit angst voor aansprakelijkheid na een van de gerechtelijke uitspraken tijdelijk stopte met het forum waarop kopers klachten konden plaatsen.[162] In deze zaak besliste de rechter op 14 februari 2009 dat Internetoplichting zich kan beroepen op artikel 6:196c BW en niet aansprakelijk is. Dat klopte niet, omdat het forum met moderatoren werkt en er in dat geval dus bemoeienis met de content is die om voor artikel 6:196c BW in aanmerking te komen juist moet ontbreken.

Op 14 maart 2009 besliste de rechter anders. Terecht werd geconcludeerd dat artikel 6:196c BW niet van toepassing kan zijn, omdat de forumbeheerder actieve bemoeienis heeft met de content. Toch gaat ook hier de rechter in de fout.

Vastgesteld moest worden of de beheerder van het forum Internetoplichting aansprakelijk kan worden gesteld. Gezien de betrachte zorgvuldigheid (o.a. kreeg Trendylaarzen binnen een uur na opening van de thread een kennisgeving hiervan, is er een stappenplan ontwikkeld waar meldingen van oplichtingen aan moeten

[162] Zie annotatie N.M. Voogd in *Tijdschrift voor Internetrecht* 2009/3 en http://jurel.nl/2009/03/21/trendylaarzen-vs-internetoplichting-4-weken-2-tegenstrijdige-vonnissen-van-vzr-amsterdam-allebei-onjuist/

voldoen zoals aangifte bij de politie, etc.) kan niet echt gesproken worden van onrechtmatig handelen. De rechter legt de lat te hoog door te bepalen dat Internetoplichting de feiten niet aannemelijk heeft weten te maken. Ook het aanbod om e-mail en IP-adressen te verstrekken vindt de rechter niet genoeg. De overweging dat misbruik van een dergelijke site gemaakt kan worden om een bedrijf te duperen is terecht. In dat geval zou zolang de forumbeheerder voldoende zorgvuldig is, enkel de plaatsers van de berichten moeten worden aangepakt (met hulp van de beheerder) en niet de beheerder.[163]

6.2.3 Aanpassing artikel 6:196c BW

Een mogelijke oplossing zou zijn om artikel 6:196c BW aan te passen, zoals Engelfriet voorstelt:[164]

> Wanneer een dienst van de informatiemaatschappij bestaat in de opslag en doorgifte van door afnemers aangeleverde informatie, is de dienstverlener niet aansprakelijk voor de op verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat:
>
> a) de dienstverlener zich afdoende inspant om via de dienst verspreide informatie die kennelijk onrechtmatig is te verwijderen of de toegang daartoe onmogelijk te maken,
> b) de dienstverlener een adequaat mechanisme hanteert waarmee derden eenvoudig een klacht kunnen indienen over door een afnemer geplaatste informatie, en
> c) de dienstverlener na een onmiskenbaar juiste klacht prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken.

Door de toevoeging sub a ontspringen achteroverleunende forumbeheerders niet langer de dans. Daarnaast kan de zich serieus voor haar geranium-forum inspannende vrouw van middelbare leeftijd door een beroep op sub a niet langer aansprakelijk worden gesteld voor eventueel op het forum geplaatste foto's die inbreuk maken of andere onrechtmatige content. Een dergelijk bepaling zou voor Web 2.0 dienstverleners in het algemeen bijdragen aan

[163] Zie paragraaf 9.1.1 voor latere uitspraken in deze zaak, waar het beter voor Internetoplichting afliep.
[164] A. Engelfriet, Naar een passend beschermingsregime voor forumbeheerders en bloggers, *Tijdschrift voor Internetrecht* 2009/3.

het ook in de toekomst kunnen blijven aanbieden van hun diensten zonder angst voor onverwachte aansprakelijkheid.

6.3 Online veilingen

Het is niet de eerste toepassing waar je bij Web 2.0 aan denkt, maar online veilingsites vallen hier ook onder. De gebruikers bepalen immers wat er, binnen de door de veilingsite ter beschikking gestelde infrastructuur, gebeurt. Op bijzonder grote schaal worden gebruikers van online veilingsites aansprakelijk gesteld voor geleden schade. De aanbieders van de veilingdienst worden minder aangesproken, maar de inzet van deze conflicten kan bijzonder groot zijn. Hoewel het model meer wegheeft van een grote online vlooienmarkt, wordt Marktplaats de grootste veilingsite van Nederland beschouwd. Om die reden is Marktplaats ook opgekocht door eBay, die wereldwijd marktleider is als aanbieder van online veilingen. Hieronder zullen kort enkele in der loop der tijd ontstane conflicten besproken worden.

Binnen het internetrecht is Marktplaats vooral bekend door de zaak die Stokke, de producent van onder andere een speciaal type baby/peuter-stoel, de zogenaamde TRIPP TRAPP stoel, heeft gevoerd.[165] In deze uitspraak is bepaald dat Marktplaats aanbiedingen niet vooraf hoeft te screenen en deze ook niet binnen 24 uur na plaatsing hoeft te verwijderen. Marktplaats heeft een goede notice- en takedown procedure en het is aan degene op wiens merk inbreuk wordt gemaakt de aanbieder daarvan op de hoogte te stellen.

Markplaats komt in de rechtspraak daarnaast regelmatig terug (tientallen keren per jaar) wegens oplichtingspraktijken van aanbieders op de veilingsite.[166] In die gevallen blijft de site zelf buiten schot en gaat het uitsluitend om de via de Marktplaats-infrastructuur verlopende handel.

In het bekende Pesser/Lycos-arrest[167] is er een oordeel gegeven over wanneer een hosting-provider de NAW-gegevens aan een

[165] Rechtbank Zwolle, 3 mei 2006, LJN AW6288.
[166] Zie recent onder andere Rb. Arnhem 2 juni 2010 (LJN BM6703) waarin een veroordeling van 2 jaar (waarvan 1 voorwaardelijk) is uitgeproken wegens bestelde en niet geleverde iPods en Hoge Raad 25 mei 2010, LJN BL5625 over verkoop van een gestolen fiets.
[167] Hoge Raad 25 november 2005, LJN AU4019.

derde dient af te geven. Hierover is veel geschreven, de reden om de zaak hier aan te halen is dat de aanleiding voor dit arrest de handel in postzegels op eBay was. Op een site die gehost wordt door Lycos wordt de postzegelhandelaar in een negatief daglicht gezet. De naam van de site was stopthefraud en een van de teksten was: "have you ever been ripped off by…" gevolgd door de naam van de postzegelhandelaar. De postzegelhouder sommeert Lycos om de site te verwijderen en de NAW-gegevens van de persoon achter de website bekend te maken. Lycos weigert mee te werken. Zowel de rechtbank als het Hof concluderen dat Lycos de NAW-gegevens bekend dient te maken. De Hoge Raad beslist dat het Hof geen onjuiste maatstaf heeft gehanteerd omdat het een nauwgezette afweging gemaakt heeft van alle betrokken belangen, waaronder het belang van de bescherming van de persoonlijke levenssfeer van de websitehouder.

Hoewel er prachtige conflicten over de verkoop van foto's in plaats van telefoons bij de niet erg tactvolle Judge Judy zijn voorgekomen,[168] worden de meeste eBay conflicten via hun eigen conflictoplossingsdienst opgelost. Meer dan 60 miljoen conflicten worden per jaar afgehandeld,[169] waarvan de meerderheid (80-90%) enkel via directe onderhandeling tussen de conflicterende partijen, enkel ondersteund door de techniek. In eerste instantie had eBay dezelfde houding als Marktplaats, namelijk dat ze een derde zijn die een infrastructuur voor handel aanbieden en dat daaruit voortvloeiende conflicten voor de verantwoordelijkheid van de gebruikers komen. Door het grote aantal conflicten merkte eBay dat het voor het bedrijf beter was als deze goed werden opgelost. Om die reden begon men aan de ontwikkeling van een geschillenoplossingsdienst. Marktplaats zal mogelijk in de toekomst dezelfde stap zetten.

eBay heeft veel last van handel in artikelen die inbreuk maken op merkrechten. In april 2010 werd eBay in Amerika niet verantwoordelijk gehouden voor merkinbreuk op juwelen van Tiffany.[170] Minder gelukkig was eBay in een door Louis Vuitton aangespannen

---

[168] Zie *eBay Scammer on Judge Judy*, http://www.youtube.com/watch?v=ZJDK6ctRjqw en *Judge Judy - Scam victim scams a buyer on ebay*, http://www.youtube.com/watch?v=RpfDoK0-Pe0.

[169] Zie 16 miljoen eBay/Paypal-conflicten per jaar: "We can work it out" of "Let it be"? http://lodder.cli.vu/flits/flits10.html en http://jurel.nl/2010/01/20/e-courtnl-%E2%80%93-enkele-kanttekeningen-bij-een-boeiend-initiatief/

[170] *EBay found innocent in counterfeit jewelry appeal*, http://www.betanews.com/article/EBay-found-innocent-in-counterfeit-jewelry-appeal/1270147654

zaak wegens merkinbreuk voor de Parijse rechter, die in november 2009 een boete van 1,7 miljoen euro oplegde.[171]

[171] http://www.guardian.co.uk/technology/2009/nov/30/ebay-louisvuitton-perfume

7 Openbaarheid: smaad en onrechtmatige uitingen

Openbaarheid is een typisch internetrecht-concept, dat afhankelijk van de juridische domein (auteursrecht, vrijheid van meningsuiting, smaad, etc.) verschillend wordt uitgelegd.[172] Internetrecht juristen kunnen vanuit hun internet invalshoek, die specifieke juridische disciplines overstijgt, een bijdrage leveren aan eenheid in de uitleg van het concept openbaarheid op internet.

Internet is een netwerk met - zeker van oorsprong - in beginsel voor een ieder toegankelijke informatie. Daarop zijn steeds meer uitzonderingen. Waar in het verleden slides van colleges via openbare websites werden verspreid, gebeurt dit nu via besloten digitale leeromgevingen als Blackboard. En waren krantenberichten ooit voor iedereen toegankelijk, tegenwoordig hebben kranten een archief waar alleen tegen betaling van gebruik gemaakt mag worden.[173] In de regel geldt dat voor een beperkte groep toegankelijke informatie niet openbaar is. Zo is het uploaden van auteursrechtelijk beschermde content (zoals MP3-bestanden van populaire artiesten) niet toegestaan op een P2P-netwerk (openbaar), maar wel in de beslotenheid van een online muziekzaak (bijv. bol.com).

Communicatie op internet is doorgaans besloten. E-mail en chat berichten zijn enkel bestemd voor de beoogde ontvanger(s). Bij discussiegroepen is het mogelijk dat pas na inschrijving toegang worden verleend (besloten), maar ook voor een ieder te bekijken discussiegroepen bestaan (openbaar). Dit laatste voorbeeld illustreert de complexiteit van het begrip beslotenheid wanneer dit op internet wordt toegepast. Als immers *iedereen* zich in kan schrijven, schuift een besloten discussiegroep erg in de richting van openbare omgeving. Ook 1-op-1 besloten communicatie kan, zelfs in de offline wereld, tot openbaarheid van informatie leiden. Voor de Wet openbaarheid van bestuur geldt "openbaar voor één, is

---

[172] Zie 'Inleiding' in T. van der Linder-Smith & A.R. Lodder (2009), *Jurisprudentie Internetrecht Annotaties*, Deventer: Kluwer.

[173] *I Got Dem Ol' Cozzmoss Blues Again Mama! – over optimaliseren van de opbrengst van online publicatie van auteursrechtelijke werken,* http://jurel.nl/2009/08/12/

openbaar voor een ieder." Als informatie aan één persoon is verstrekt, is het daarmee openbaar.

Als laatste voorbeeld online geschillenoplossing, waarbij zowel mediation als arbitrage besloten is. Alles wordt in vertrouwen gezegd en *mag* niet naar buiten gebracht worden.[174] Ultieme beslotenheid, smaad is uitgesloten. Stel dat er binnen de online omgeving een muziekje gedraaid wordt om de strijdende partijen goede zin te geven. Auteursrechtelijk gezien is hier waarschijnlijk toch sprake van een openbaarmaking en zijn er rechten verschuldigd.

Waar moeten we een *besloten* Hyves-profiel plaatsen? Is het te vergelijken met online geschillenoplossing, algemene informatie of besloten communicatie? Welke factoren spelen een rol om te bepalen of een 'smadelijke' uiting is gedaan, dus "met het kennelijke doel om daaraan ruchtbaarheid te geven"? Het lijkt dat ten aanzien van Web 2.0 toepassingen een bredere opvatting van openbaarheid wordt gehanteerd dan in de fysieke wereld. Dit brengt met zich mee dat uitlatingen via een Web 2.0 toepassing eerder als onrechtmatig beschouwd kunnen worden dan uitlatingen in de fysieke wereld.

In dit hoofdstuk beperken we ons tot openbaarheid in relatie tot Hyves-profielen. Hierbij wordt ingegaan op onrechtmatige uitingen binnen het strafrecht, smaad derhalve. Dit onderwerp is met name interessant omdat eind 2009 twee gerechtshoven (Leeuwarden en Den Bosch) hierover verschillend oordeelden.[175]

7.1 Smaad bij de rechtbank Assen 2008

De vraag is of een opgerekt openbaarheidbegrip niet als een disproportionele beperking van het recht op vrijheid van meningsuiting (artikel 2 Gw) moet worden gezien. Zou er ten aanzien van

[174] Zie onder andere de dissertaties van S.H. Bol (2007), *Mediation en Internet. Analyse van juridische regels en noodzakelijke waarborgen voor mediation op internet* (VU Amsterdam 2007), SDU uitgevers, S. Schiavetta (2008), *Electronic Alternative Dispute Resolution – Increasing Access to Justice vai Procedural Protections*, Oslo dissertation series no. 7 en P. Cortes (2010), *Online Dispute Resolution for Consumers in the European Union*, Routledge - Research in Information Technology and E-commerce Law (diss. Cork 2008).

[175] Bij dit hoofdstuk is gebruik van gemaakt de in Tijdschrift Internetrecht 2010/1 verschenen annotatie.

Web 2.0 toepassingen niet een ander/minder streng openbaarheidsbegrip gehanteerd moeten worden? Zeker nu gebruikers van dergelijke sites veelal hun uitlatingen vanuit de beslotenheid van hun fysieke huiskamer op internet zetten.

7.1.1 De huiskamer als metafoor

De huiskamer is binnen de rechtspraak rondom smaad een veel gebruikte metafoor. Het volgende voorbeeld kan verhelderend werken. Stel dat vanuit de huiskamer een persoon enkele uitingen doet, terwijl het raam open stond. Zijn hiermee deze uitingen in het openbaar gedaan? De meeste gebruikers van Web 2.0 toepassingen zullen zich er van bewust zijn dat iedere internetgebruiker toegang kan krijgen tot deze informatie. Dit geldt in wezen ook voor de spreker in de woonkamer met open raam. Het illustreert wel dat het criterium streng is.

In de Martijn-zaak[176] uit 2007 kwam de rechter niet toe aan het formuleren van criteria waaronder op internet sprake is van beslotenheid. In de zomer van 2008 bepaalde de Rechtbank Assen dat zelfs een besloten Hyves-profiel openbaar is.[177] In casu ging het om een vrouw die over haar ex op een besloten Hyves-profiel meldde dat ze het vervelend vond haar kind met deze pedofiel te moeten meegeven. Volgens de man werd hij sindsdien met de nek aangekeken en genoopt te verhuizen. Het is op zich verbazend dat dergelijke uitingen over een ex klakkeloos worden geloofd. Negatieve uitingen over zijn/haar ex behoren doorgaans niet tot de meest waarheidsgetrouwe.

7.1.2 Bestaat beslotenheid op internet?

Het fenomeen roddel en achterklap bestond natuurlijk al lang voor het internet. Uitingen op internet krijgen al snel de status van het schreeuwen vanaf een zeepkist in een druk park (= openbaar). De vraag is of er nog ruimte is voor stillere plekjes die lijken op een huiskamer of een wandeling met je vriend door het bos (= besloten)?

Wanneer je in een mailtje aan 5 vrienden vertelt dat je ex een pedofiel is, dan lijkt dit niet onder smaad (artikel 261 Sr) te kunnen vallen. Met "ruchtbaarheid geven" uit lid 1 van dit artikel

[176] Vzr. Amsterdam 1 november 2007, LJN BB6926.
[177] http://jurel.nl/2010/03/22/cassatie-besloten-hyves-profiel-en-kastje-naar-de-muur-rb-assen-vonnis/

wordt bedoeld "het ter kennis van het publiek brengen".[178] Met zodanig 'publiek' is een bredere kring van betrekkelijk willekeurige derden bedoeld.

Bij openbare Hyves-profielen blijkt het etiket 'vrienden' niet al te serieus genomen te hoeven worden, zoals in het openingsnummer van *Tijdschrift voor Internetrecht* 2008/1 opgemerkt, zat een van de Hyves-vrienden van Balkenende eind 2007 vast wegens bedreiging van zijn vriend (lees: Balkenende) op internet.[179]

7.1.3 Betrekkelijk willekeurige derden

Een zorgvuldig beheerd besloten Hyves-profiel (met hooguit enkele tientallen ECHTE vrienden en kennissen) zou als besloten in de zin van artikel 261 Sr kunnen worden gekwalificeerd. Een uiting op een verjaardag kan immers ook niet als smaad worden gezien. Het probleem met internet is dat vrijwel alle beslotenheid in beginsel bereikbaar is voor een ieder. Ook op een zorgvuldig onderhouden besloten Hyves-profiel kunnen "betrekkelijk willekeurige derden" zich melden, alleen al omdat iemand gemakkelijk op Hyves de identiteit van een ander kan aannemen.

Blijft eigenlijk alleen over individuele communicatie. Stel je bent aan het chatten met 10 ECHTE vrienden en zegt dat je ex een pedofiel is. Wat dan? Lastig, omdat ook hier geldt dat er onbedoeld een "betrekkelijk willekeurige derde" onder de 10 vrienden kan blijken te zitten.

Bij smaad zul je als partij bewijs moeten leveren dat het bedoelde forum ECHT besloten was. Schuldig totdat je onschuld bewezen is. Het is niet anders. Spreek dus maar beter geen kwaad over anderen op internet.

7.1.4 Persoonlijke aard van de uiting

Blijft over nog een ander punt. De aard van de uiting. Als er op een 'besloten' Hyves-profiel melding over een ex gedaan wordt, is het enkel voor degenen die van het bestaan van de voormalige relatie afwisten duidelijk wie er bedoeld wordt. Het is echter mogelijk om achteraf te achterhalen wie de ex is en zelfs als die mogelijkheid niet bestaat, blijkt de kans niet uitgesloten dat er "be-

[178] HR 22 januari 1965, NJ 1965, 131
[179] Hoge Raad 15 december 2009, LJN BJ7237.

trekkelijk willekeurige derden" ook afweten van de voormalige relatie.

Zijn we monddood op internet en moeten we oppassen bij alle krabbels op Hyves en andere plekken? Niet echt. Het grondrecht "vrijheid van meningsuiting" laat betrekkelijk veel ruimte open, maar bij dergelijke persoonlijke uitingen als die over een ex is op het internet terughoudendheid geboden.

7.2 Smaad bij twee gerechtshoven 2009

Eind 2009 zijn twee uitspraken gedaan door de gerechtshoven Den Bosch en Leeuwarden (dit is het appel van de hierboven besproken Rechtbank Assen zaak). In deze uitspraken werd de vraag of een besloten gebruikersprofiel op een sociale netwerksite als openbaar moet worden gezien zowel bevestigend als ontkennend beantwoord.

7.2.1 Opzettelijke aanranding eer

Om te kunnen spreken van smaad moet om te beginnen opzettelijk iemands goede naam of eer worden aangerand door telastlegging van een bepaald feit. Het doet er daarbij niet toe of het waar is wat wordt gezegd, behalve dat als de aanrander weet dat het *niet* waar is er sprake is van het zwaarder bestrafte laster (artikel 262 Sr). In de zaak van het Hof Leeuwarden noemt de verdachte haar ex-partner een pedo, in de zaak van het Hof Den Bosch de verdachte zijn broer een oplichter. Van beide kwalificaties kan worden gesteld dat ze duidelijk een aanranding vormen van iemands goede naam of eer.

7.2.2 Ruchtbaarheid geven

De centrale rechtsvraag in zaken van het Hof Den Bosch en het Hof Leeuwarden is of het mogelijk is om via een besloten Hyvesprofiel "ruchtbaarheid te geven" aan de gememoreerde weinig vleiende bewoordingen. De openbaarheid in de zin van smaad bestaat uit het communiceren met "een bredere kring van betrekkelijk willekeurige derden." Bij online geschillenoplossing zijn er geen betrekkelijk willekeurig derden. Bij een krantenarchief ook niet. Ook chat- en e-mail communicatie is niet bestemd voor willekeurige derden.

7.2.3 Zorgvuldig toegangsbeleid

Crux is hoe zorgvuldig het toegangsbeleid is. In de regel wordt aangenomen dat een huiskamer een dergelijk zorgvuldig toegangsbeleid kent. Een ieder die daar komt, wordt geacht niet tot betrekkelijk willekeurige derden te behoren. Is een besloten Hyves-profiel hiermee te vergelijken?

Hoe waren de profielen samengesteld? In de Bossche zaak verklaarde de verdachte:

> "(…) dat slechts 10 à 12 personen – voornamelijk familieleden – de betreffende teksten en foto konden bekijken. Voor andere Hyves-gebruikers waren deze teksten en foto volgens hem niet zichtbaar."

Op basis hiervan concludeert het Hof dat de verdachte de gewraakte berichten niet ter kennis heeft gebracht aan een bredere kring van betrekkelijk willekeurige derden, maar aan een beperkt aantal selecte personen. Wat opvalt is dat enkel de kwantiteit (10-12) en kwaliteit (voornamelijk familieleden) een rol lijkt te spelen. Op *hoe* deze groep precies wordt beheerd wordt niet ingegaan. Hier had de rechter wel aandacht aan moeten besteden, want uit de weergegeven feiten is niet duidelijk dat er *geen* betrekkelijk willekeurige derde tussen de Hyves-vrienden zou kunnen zitten.

In zaak van het Hof Leeuwarden gaf de verdachte aan:

> "dat de betreffende Hyves-pagina (…) slechts toegankelijk was voor door verdachte toegelaten, circa 20 à 25, "Hyves-vrienden". Volgens verdachte waren dit familieleden, vrienden en bevriende ex-collega's."

Waar in Den Bosch sprake is van *voornamelijk* familieleden en de status van de overige vrienden niet uit het vonnis blijkt, is hier in ieder geval duidelijk dat de groep Hyves-vrienden gemakkelijk op een feestje in de woonkamer zouden kunnen aanschuiven zonder dat er zich betrekkelijk willekeurige derden in de menigte zouden mengen. Ook hier overigens geen overwegingen over het toelatingsbeleid, enkel een stelling over wie er volgens de verdachte deel uitmaken van de Hyves-vrienden. Het Hof komt echter tot een tegenovergestelde conclusie:

> "de wijze waarop -en de aard van de bewoordingen waarin- verdachte haar gedachten via haar Hyves-pagina met een

> twintigtal anderen heeft gedeeld niet anders worden opgevat dan het welbewust en derhalve opzettelijk ruchtbaarheid geven aan die uitlatingen. Het betrof immers niet een beperkt aantal geadresseerden die -zoals de raadsman de vergelijking maakt- in de beslotenheid van de huiskamer vertrouwelijke informatie krijgt toevertrouwd."

Deze redenering is niet goed te volgen. Waarom zou de kring in de huiskamer uit anderen bestaan dan familieleden, vrienden en bevriende ex-collega's? Als je dezelfde groep offline plaatst had het wel gekund? Wat ontbreekt is zoals al eerder aangegeven een overweging over *hoe* het profiel beheerd is. Pas dan kan de huiskamer-metafoor al dan niet ter zijde geschoven worden.

7.2.4 Geen online huiskamer

Het Hof stelt dat het geen met een huiskamer vergelijkbare situatie is op grond van de volgende drie overwegingen.

1. *De kring is in potentie ruimer*

Dit is op zichzelf juist. Het aantal personen dat in potentie toegang tot een profiel kan krijgen van een sociale netwerksite is vele malen groter dan die in een willekeurig huiskamer passen. De vraag die niet beantwoord wordt is wie van de Hyves-vrienden dan *niet* deel zouden kunnen uitmaken van een in de huiskamer aanwezige groep. Dit hangt af van de wijze waarop 'vrienden' geselecteerd worden.

2. *Men "kennelijk naar eigen inzicht en zonder enige restrictie over de uitlatingen mocht beschikken"*

Is een dergelijke clausule tijdens roddel en achterklap in de omgeving van de huiskamer gebruikelijk? Wordt er gewaarschuwd "niet doorvertellen hoor" en maakt een dergelijk clausule juridisch gezien verschil? Mogelijk dat de Rb. Assen zaak meer helderheid had kunnen verschaffen over de feitelijke toedracht (maar dus zoals gezegd niet te vinden op Rechtspraak.nl), want enkel wordt duidelijk dat de verdachte in een online dagboek aangeeft haar kinderen niet met die pedo te willen meegeven. Een dagboek is een verslaglegging met veelal emotionele kleuring waarbij de lezer dergelijke uitspraken zou moeten kunnen nuanceren. Dat de ex als gevolg van deze uitingen zo onheus werd benaderd dat hij zich genoodzaakt voelde te verhuizen is bijzonder vervelend, maar ligt meer aan de ontvangers van het bericht over de vermeende eigenschappen van deze man dan aan de verzender.

3. *"waarbij daarnaast een verdere verspreiding van de gewraakte tekst door de oorspronkelijk geadresseerden -gezien de aard van de beschuldiging- voor de verdachte niet alleen in theorie voorzienbaar was maar ook op voorhand feitelijk te verwachten viel."*

> Deze overweging schiet te ver door. Zoals aangegeven wordt hier door een ex een bepaalde kwalificatie gegeven. Is dan feitelijk te verwachten dat dit gerucht zich verder verspreid? Het zegt veel over de geadresseerden, maar als hiermee rekening moet worden gehouden is het zelfs mogelijk dat tijdens online geschillenoplossing of 1-op-1 communicatie gedane uitingen *ook* smaad kunnen zijn. Dat kan toch niet de strekking van "ruchtbaarheid geven aan" zijn.

7.2.5 Belediging

In de zaak van het Hof Den Bosch wordt nog ingegaan op het subsidiair ten laste gelegde belediging. Hierbij wordt 'openbaarheid' expliciet genoemd: "(…) nu de gewraakte uitlatingen zijn gedaan op een website die slechts toegankelijk was voor een gering aantal selecte personen, deze niet in het openbaar zijn gedaan. Evenzeer volgt hieruit dat het opzet van verdachte niet was gericht op openbaarheid." Daargelaten dat de website (Hyves) voor iedereen toegankelijk is, speelt voor het besloten profiel zowel het aantal (gering) als het type (selecte). Zelfs een groep van 30 man (vgl. een ruim bemeten woonkamer) zou select kunnen zijn. Het Hof Leeuwarden had minder nadruk op de hoeveelheid personen en de aard van de uiting moeten leggen, en nader dienen in te gaan op hoe zorgvuldig het profiel beheerd is.

7.3 Slotopmerkingen

De uitspraken van beide hoven zijn wat de uitkomst betreft tegengesteld, maar kunnen op zichzelf juist zijn. Door ontbrekende motivering op het cruciale punt van de selectie wordt niet helder of dit ook het geval is. De conclusie dat een profiel met 10-15 vrienden als besloten wordt gezien en met 25-30 als openbaar lijkt een kwantitatieve grens te suggereren die ergens tussen de 15-25 ligt. Dit is echter niet een werkbaar criterium om te bepalen of informatie of communicatie op het internet openbaar is. Er zijn wel grenzen. Zoals de suggestie van een IT professional dat haar LinkedIn profiel met 1000 contacten zeer zorgvuldig beheerd wordt. Hoewel dit mogelijk is, moeten uitingen in dat geval toch zonder-

meer geacht worden in het openbaar te zijn gedaan. In een andere context komt hieronder nog een profiel aan de orde met bijna 100 personen (paragraaf 9.2.3). Dat aantal komt zeker in de buurt van een kwantitatieve grens.

De aard van de uiting in de zin van de te verwachten verspreiding (hoe ernstiger, hoe eerder/meer) dient hooguit een ondergeschikte rol te spelen.

Bepalend moet zijn de wijze waarop het "toelatingsbeleid" is vormgegeven. Een zorgvuldig beheer kan eruit bestaan dat bijvoorbeeld bij de lijst van Skype-contacten iemand enkel wordt toegevoegd na webcam-contact. Hiermee kan worden voorkomen dat zich onder de groep betrekkelijk willekeurige derden bevinden.

Indien in (een van) beide zaken gecasseerd wordt, is te hopen dat de Hoge Raad deze lijn volgt en dan waarschijnlijk wegens feitelijke onduidelijkheid zal terugverwijzen.

8 Privacy

De Wet bescherming persoonsgegevens (Wbp) is een uitwerking van de in 1995 vastgestelde EU Richtlijn 95/46 inzake de bescherming van persoonsgegevens. Midden jaren negentig was de invloed van het internet op de samenleving beperkt en er is dus niet expliciet met het internet rekening gehouden. De definitie van de centrale concepten (verantwoordelijke, bewerker, persoonsgegeven) is echter technologie-neutraal. Hierdoor kunnen nieuwe ontwikkelingen onder het toepassingsbereik van de wet worden gebracht, maar dit leidt niet altijd tot een bevredigend resultaat.

Een in dit licht sprekend voorbeeld is de Lindqvist-uitspraak van het Hof van Justitie in 2003. Bodil Lindqvist beheerde een weblog met wetenswaardigheden over haar kerkgenootschap en werd meldingsplichtig geacht. Naar de letter van de Richtlijn 95/46/EG juist, want een ieder die persoonsgegevens verwerkt, in de zin van tot individuele personen herleidbare informatie, valt in beginsel onder de wet. Naar de geest van de richtlijn is dit onjuist. Het is en kan immers nooit de bedoeling zijn om individuen die tot de persoon herleidbare wetenswaardigheden op een internetsite plaatsen lastig te vallen met het specificeren van een doel voor de verwerking, hem aan dat doel gebonden te achten en hem te verplichten deze verwerking aan te melden.

Grondrechten, zoals privacy in artikel 8 EVRM, zijn uit hun aard als algemene beginselen verwoord en om die reden robuuster en beter tegen de ontwikkelingen zoals het internet en de in dit boek centraal staande Web 2.0 toepassingen bestand dan de Wbp. Het EVRM moet echter wel per situatie worden geïnterpreteerd en hierdoor is het een instrument dat niet gemakkelijk kan worden ingezet. Daarnaast kan het alleen worden ingeroepen tegen overheden, dus wat dat kan de Wbp de burger uitkomst bieden bij een conflict met een bedrijf.

In dit hoofdstuk zullen enkele privacy-aspecten van Web 2.0 worden behandeld. Eerst wordt kort ingegaan op de Richtsnoeren van de Cbp voor persoonsgegevens op internet. Daarop voortbouwend wordt de zorgplicht van artikel 11 Wbp besproken. In de paragrafen 8.3-8.7 worden enkele voor privacy relevante kwesties be-

sproken, te weten overlijden, bewustwording, sollicitaties, persoonlijke informatie van jongeren en spam via krabbels.

8.1 Richtsnoeren Cbp: persoonsgegevens op internet

In de *Richtsnoeren Publicatie van persoonsgegevens op internet*[180] staan richtlijnen van het Cbp over wat wel of niet toelaatbaar is op het terrein van publicaties op internet. In de richtsnoeren is het als volgt verwoord:[181]

> "De richtsnoeren behandelen veel van de belangrijkste regels op het gebied van de bescherming van persoonsgegevens maar bevatten geen uitputtende beschrijving van alle bestaande wettelijke bepalingen en jurisprudentie."

Er wordt dus duidelijk ruimte gelaten voor interpretatie. Allereerst rijst de vraag: wat wordt verstaan onder een persoonsgegeven? Artikel 1 sub a Wbp luidt als volgt: "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon." Hoe is dit nu op het internet?

Hierbij wordt uitgegaan van het IP-adres.[182] Het IP-adres zal echter in beginsel niet verder te herleiden zijn dan tot de provider. Deze kan dan vervolgens desgewenst nagaan welke klant gebruik heeft gemaakt van het betreffende IP-adres op dat specifieke tijdstip. Deze gegevens mogen de providers echter niet 'zomaar' aan derden ter beschikking stellen. Het Hof Amsterdam oordeelde in 2006[183] dat service providers niet gehouden zijn om schriftelijke opgave te doen van namen en adressen van de abonnees aan wie IP-adressen zijn toegekend. Een maand later oordeelde de rechtbank in Amsterdam echter dat een service provider gehouden kan zijn om abonneegegevens te verstrekken.[184] Wel moet daarbij voldaan zijn aan twee voorwaarden: er dient sprake te zijn van inbreukmakend handelen en er mag geen misverstand over bestaan dat de persoon achter het IP-adres ook daadwerkelijk de persoon is die de inbreuk heeft gemaakt.

[180] http://www.cbpweb.nl/Pages/rs_publicatie_persgeg_internet.aspx
[181] *Richtsnoeren Publicatie van persoonsgegevens op internet,* p. 3.
[182] Ten overvloede, uniek en identificerend nummer waarmee een computer via een provider toegang krijgt/heeft tot het internet.
[183] Gerechtshof Amsterdam 13 juli 2006, LJN AY3854.
[184] Rechtbank Amsterdam 24 augustus 2006, LJN AY6903.

Volgens artikel 1 sub a Wbp dient er sprake te zijn van een 'natuurlijk persoon', echter, wat nu indien het IP-adres aan een rechtspersoon toebehoort? De richtsnoeren lossen dat als volgt op:[185]

> "Dat het IP-adres in sommige gevallen naar een rechtspersoon leidt, in plaats van naar een natuurlijk persoon, doet niet af aan het feit dat het in de meeste gevallen wel degelijk om persoonsgegevens gaat en dat dus de hele verzameling moet worden behandeld conform de uitgangspunten van de Wbp."

Het IP-adres wordt dus ook dan gezien als persoonsgegeven. Dit uitgangspunt stemt voor het overige in deze richtsnoeren bepaalde niet erg hoopvol. Het doel van de richtsnoeren van het CBP is onder andere om beheerders van profielensites regels op te leggen die de negatieve gevolgen moeten beperken van het feit dat de informatie op sociale netwerksites wereldwijd toegankelijk is.

De richtsnoeren getuigen op zich van moed en de gegeven voorbeelden zijn zondermeer verhelderend. Ook zijn er nuttige handreikingen voor de plaatser van persoonlijke informatie in opgenomen. Het uitgangspunt is zoals begrijpelijk de Wbp. Het Cbp zou het niet moeten willen, en zal het zeker niet aankunnen, dat alle eigenaren van een profiel op een sociale netwerksite hun verwerking zouden aanmelden. De in de richtsnoeren aangekondigde uitzondering op de meldingsplicht is begin 2010 voorzover ons bekend nog niet gerealiseerd.

8.2 De zorgplicht van artikel 11 Wbp

Op grond van artikel 11 Wbp hebben verantwoordelijken een zorgplicht voor de juistheid van persoonsgegevens. De vraag is of deze bepaling relevant is voor de op een sociale netwerksite geplaatste informatie. Als een gebruiker aangeeft een in 1982 geboren Italiaanse man te zijn en in werkelijkheid is het een in 1987 geboren Duitser, kan je dit de aanbieder van de sociale netwerksite onmogelijk aanrekenen. Het hangt ook af van de gebruiksvoorwaarden van de site, maar in de regel wordt niet verlangd om de

[185] Cbp, *Richtsnoeren publicatie van persoonsgegevens op internet*, p. 10. Zie http://www.cbpweb.nl/Pages/rs_publicatie_persgeg_internet.aspx

profielen naar waarheid in te vullen. Wel is het vanwege het doel van dergelijke sites niet voor de hand liggend om met een fake-identiteit te werken, omdat dan je echte vrienden en bekenden je niet kunnen vinden zonder aanvullende informatie. Daarentegen zijn er personen die profielensites misbruiken om, gebaseerd op een verkeerd beeld dat ze van zichzelf schetsen, in contact te komen met andere mensen.

Bij sociale netwerksites levert deze bepaling van artikel 11 Wbp weinig problemen op, de persoonsgegevens zijn immers door de deelnemer(s) zelf verstrekt. De aanname dat deze informatie daadwerkelijk afkomstig is van de gebruikers zelf, blijkt in de praktijk echter niet altijd juist te zijn. Toch kan in die gevallen moeilijk de aanbieder van de site voor de onjuiste informatie verantwoordelijk worden gehouden, eenvoudigweg omdat deze onmogelijk kan vaststellen of de door gebruikers ter beschikking gestelde persoonlijke informatie juist is.

8.2.1 Subjectieve persoonsgegevens

Hoewel persoonsgegevens doorgaans feitelijk van aard zijn, geeft de Artikel 29 Werkgroep aan dat persoonsgegevens ook subjectief kunnen zijn.[186] Dit komt er in de praktijk op neer dat ook de mening van bijvoorbeeld Jeroen de Kreek over Jan-Peter Balkenende als persoonsgegeven kan worden opgevat.[187] Hetzelfde geldt voor de befaamde "krabbel" die iemand op het Hyves-profiel van een ander kan achterlaten. Bij de juistheid van de "gegevens" (lees: meningen) die anderen over iemand geven, en die de beeldvorming om die persoon kunnen beheersen, zijn dikwijls vraagtekens te zetten.

8.2.2 Moderatie en monitoring

Handhaving van de zorgplicht van artikel 11 Wbp is in de praktijk niet werkbaar. Dit zou immers inhouden dat de verantwoordelijken voor de op sociale netwerksites aanwezige verzameling persoonsgegevens de informatie die door de deelnemers aan sociale netwerksites wordt aangeboden, inhoudelijk moeten nakijken. Het College Bescherming Persoonsgegevens leidt namelijk uit de zorgplicht af dat:

[186] GROEP GEGEVENSVERWERKING ARTIKEL 29, *Privacy op internet - Een geïntegreerde EU-aanpak van on-linegegevensbescherming*, 5063/00/NL/DEF, WP 37.
[187] Zoals bekend is dit de veroordeelde 'stalker'.

> "beheerders van sociale sites een plicht tot monitoren en *preventief* screenen van bijdragen hebben: 'verantwoordelijken dienen ervoor te zorgen dat bijdragen alleen gepubliceerd worden op tijdstippen dat er moderatie aanwezig is."

Met de moderatie lijkt het CBP te bedoelen dat er toezicht door de verantwoordelijke dient te zijn, op de door de deelnemers gepubliceerde informatie. De verantwoordelijke dient er klaarblijkelijk voor zorg te dragen dat gebruikers slechts informatie over zichzelf, of over anderen die met die informatie getraceerd kunnen worden (zelfs als deze puur subjectief is) publiceren indien de verantwoordelijke:

- daar op dat moment toezicht over heeft, en;
- de juistheid van deze informatie controleert.

Indien de zorgplicht dermate ver zou worden doorgevoerd, hetgeen naar de letter zou kunnen op basis van de ruime interpretatie zoals de Artikel 29 Werkgroep deze hanteert, zou de zorgplicht van artikel 11 Wbp gevolgen kunnen hebben voor de aansprakelijkheid van de verantwoordelijke. De handelingen die de zorgplicht van hem/haar verlangt geven de verantwoordelijke immers een actieve(re) rol ten aanzien van de publicatie van persoonsgegevens, in tegenstelling tot de passieve rol die hem/haar nu wordt toegedicht en die de aansprakelijkheid van de verantwoordelijke doet vervallen (behoudens melding van onrechtmatige informatie).

Het dilemma is dat enerzijds een zorgplicht voor de aangeboden informatie voor verantwoordelijken van een website een nobel streven is, maar dat het anderzijds niet fair, en simpel gezegd ondoenlijk is, voor hosts van websites om (alle) aangeboden informatie preventief te screenen en te monitoren. Nog los van het feit dat de verantwoordelijke in de meeste gevallen niet over de benodigde informatie beschikt om deze screening en monitoring uit te voeren.

8.2.3 Niet verantwoordelijk?

In het licht van privacy-regulering worden geeft Myspace aan dat zij voor de geplaatste materialen geen verantwoordelijkheid kan nemen:[188]

[188] http://www.myspace.com/index.cfm?fuseaction=misc.privacy, uit Privacybeleid MySpace.

> MySpace stelt de doeleinden vast voor het verzamelen, gebruiken en openbaar maken van de Registratiegegevens die je verstrekt en wordt als zodanig beschouwd als de verantwoordelijke voor de verwerking deze gegevens. Omdat het Lid, en niet MySpace, het doel bepaalt waarvoor de Profielinformatie verzameld, gebruikt en openbaar gemaakt wordt, is MySpace niet de verantwoordelijke voor de Profielinformatie die leden in hun Profiel plaatsen.

Het is echter de vraag in hoeverre het waar is dat MySpace niet het doel bepaalt waarvoor de informatie gebruikt wordt. De informatie wordt weliswaar door de gebruikers geplaatst, maar MySpace is de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens[189] als deze informatie vervolgens verwerkt wordt, zeker wanneer deze informatie gekoppeld wordt aan de registratiegegevens. Bovendien zal het MySpace niet helpen als ze door derden aangesproken worden over incorrecte of onrechtmatige persoonsgegevens over anderen die door deelnemers geplaatst is. Hierin zal MySpace, na marginale afweging van belangen, al dan niet tot actie over moeten gaan.

8.2.4 Artikel 11 Wbp als oplossing?

De Wbp en de toezichthouder Cbp hebben vooralsnog moeite met het internet. Dit gelft zeker ook voor sociale netwerksites. Hoe kunnen de CBP en de Wbp er voor zorgdragen dat men in het kader van sociale netwerksites up-to-date wordt? Artikel 11 Wbp zelf biedt wellicht een eerste optie voor een oplossing:

1. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.
2. De verantwoordelijke treft de nodige maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

In lid 2 wordt bepaald dat de verantwoordelijke inzake de juistheid en nauwkeurigheid van gegevens slechts de nodige maatregelen dient te treffen "gelet op de doeleinden" waarvoor de informatie wordt verzameld of verwerkt. Het doeleinde van (de gebruikers

[189] Er hierbij vanuit gaande dat ze ergens binnen de Europese Unie een vestigingsplaats hebben.

van) een sociale netwerksites is het delen van (persoonlijke) informatie met anderen. De juistheid van deze informatie doet in feite, zolang van een onrechtmatig karakter van deze informatie niet blijkt, niet ter zake. Men kan zich op het internet immers voordoen zoals men wil.

Het doeleinde van sociale websites hoeft, los van de Wbp bezien, niet in te houden dat de persoonsgegevens van de "auteur" juist en nauwkeurig zijn. Wat is anders de waarde van het recht om onder een pseudoniem te opereren. En waarom zou een deelnemer aan een sociaal netwerk, de professionele netwerken hiervan uitgezonderd, zich niet mooier of anders mogen presenteren dan in werkelijkheid? Dit geldt zeker voor de "virtueel" ingestelde sociale netwerken?

8.2.5 Minder vergaande zorgplicht

Op grond van lid 2 is er geen sprake van een verregaande zorgplicht voor sociale netwerksites. Om deze interpretatie effectief te laten zijn, dient er wel een extra vangnet geconstrueerd te worden, zodat andere sites niet op deze wijze van hun zorgplicht gekwijt worden.

Een alternatief is het toevoegen van een nieuw lid aan artikel 11 Wbp. Dit derde lid zou kunnen inhouden dat de zorgplicht als geformuleerd in lid 2 niet van toepassing is op verantwoordelijken (zowel hosts als providers) voor websites waarvan de aard meebrengt dat gebruikers van de betreffende website zelf persoonsgegevens aandragen, zulks behoudens de melding door (een) belanghebbend(en) van de onrechtmatigheid van deze persoonsgegevens.

Op deze wijze ontheft men de verantwoordelijken voor sociale netwerksites van een vergaande zorgplicht, terwijl er een slag om de arm wordt gehouden met de noodzakelijke melding door belanghebbenden. Het zijn tenslotte deze belanghebbenden die als eerste geconfronteerd zullen worden met de onrechtmatigheid van (met name subjectieve) persoonsgegevens. Om misbruik hiermee te kunnen voorkomen zou het CBP bij een melding kunnen verzoeken de desbetreffende informatie preventief te verwijderen, alvorens men nagaat of de melder een belanghebbende is en of de informatie daadwerkelijk onrechtmatig is. Op deze manier wordt een flexibele situatie gecreëerd, voor de controle en handhaving van een flexibel evoluerend vraagstuk.

8.3 Overlijden

Tijdens de GiKii 2009 was er een presentatie van Lilian Edwards getiteld death 2.0.[190] Het is niet altijd gemakkelijk om allerlei digitale sporen op internet van iemand die overleden is te verwijderen. Het gaat in dit geval niet om informatie over deze overleden personen, maar op hun naam staande e-mail accounts, sociale netwerkprofielen, etc. Zoals bekend hebben overleden personen zelf geen recht op privacy. Hoewel er argumenten zijn om privacy van een overledene te respecteren, is het Nederlandse begrip, persoonlijke *levens*sfeer, zeer direct gelinkt aan het leven van een persoon. De reden om het onderwerp in het hoofdstuk privacy te behandelen is dat de belangen die spelen gerelateerd zijn aan privacy.

8.3.1 Herdenkingspagina's

Hyves biedt de mogelijkheid om een "herdenkingspagina" van de overledene te laten voortbestaan, met foto's, krabbels, slideshows en muziek. Op www.krabbelmaar.nl kunnen nabestaanden kiezen uit talloze afbeeldingen van bloemen en kaarten, om op de pagina van de overledene zetten. Er was medio 2008 nog niets geregeld in de Algemene Voorwaarden van Hyves over het uit de lucht halen van een Hyves-profiel (evenmin in de Algemene Voorwaarden van Facebook en MySpace). Er bleek in het "businessplan" van Hyves geen rekening te zijn gehouden met het eventuele overlijden van gebruikers.

Juridisch gezien is dit een opmerkelijke kwestie, immers in de niet-virtuele wereld houdt een natuurlijke persoon op te bestaan als hij overlijdt. Er zijn dan nog slechts nabestaanden en/of erfgenamen. Een profiel op Hyves lijkt niet te vallen onder overdraagbare rechten, waartegen de wet of de aard van het recht zich niet verzet (artikel 3:83 lid 1 BW).[191] Het profiel is immers zodanig persoonlijk, met persoonlijke vrienden, hobby's, voorliefdes voor merken, etc. dat overdracht aan nabestaanden niet mogelijk lijkt. Pijnlijke bijkomstigheid kan zijn dat "vrienden" van de overledene via Hyves een bericht krijgen over een ophanden zijnde verjaardag van de inmiddels overledene met bijbehorend feestje.

[190] http://www.law.ed.ac.uk/ahrc/gikii/docs4/edwards.pdf
[191] Zie ook Eva Visser, 'Who owns your bits when you die', *Computerrecht* 2007, 113.

8.3.2 Overlijdensberichten van levenden

Behalve problematiek rond content van een voormalige levende persoon (dus inmiddels overleden), komt het ook voor dat ten onrechte iemands overlijden wordt gemeld. Enige ophef is er geweest over de website sterfdatum.nl.[192] Op deze site is het mogelijk om van een willekeurig al dan niet in werkelijkheid bestaand persoon zijn sterfdatum te laten berekenen. Aan de hand van een aantal antwoorden op vragen over de levensstijl, geboortedatum, gewicht, etc. berekent het programma de vermoedelijke sterfdatum. Behalve deze berekening wordt ook een rouwadvertentie aangemaakt en op de site geplaatst. Dit laatste kan mogelijk wel een inbreuk op de persoonlijke levenssfeer vormen. Regelmatig worden argeloze ego-surfers[193] geconfronteerd met een annonce van hun vermeende overlijden, zoals aangemaakt via sterfdatum.nl.

Stel dat de site vermeld dat Gijsbert Brunt overleden is. De huidige voorzitter van de NVvIR zou bezwaar kunnen maken, ware het niet dat de site de herleidbaarheid niet volledig heeft gemaakt. Er wordt namelijk geen geboortedatum vermeld, enkel de leeftijd op moment van overlijden en de sterfdatum. Hoewel de voorwaarden aangeven geen rouwadvertenties te verwijderen (zoals in dit voorbeeld van onze gewaardeerde voorzitter), blijken de beheerders in de praktijk dit wel te doen. Het vervelende voor de zogenaamd overledene is dat de site door Google geïndexeerd wordt en als er op de naam gezocht wordt als een van de eerste treffers de rouwadvertentie kan verschijnen. Hoewel binnen de context van de site duidelijk is dat deze advertenties ludiek bedoeld zijn, zal dit niet voor iedereen die het zoekresultaat ziet evident zijn.

Op sociale netwerksites kan ook ten onrechte melding worden gemaakt van het overlijden van een deelnemer. Regelmatig ontvangt bijvoorbeeld Hyves klachten over het uit de lucht zijn van een profiel. Bij nader onderzoek blijkt de eigenaar van het profiel dan door een derde als "overleden" te zijn gemeld.[194] Waar hierboven werd aangegeven dat medio 2008 nog niet geregeld was hoe een profielpagina van een overledene kan worden verwijderd,

[192] http://jurel.nl/2009/02/10/dodelijke-humor-sterfdatumnl/

[193] Het via een zoekmachine zoeken naar content waar de zoekende zelf in genoemd wordt.

[194] Dit zou geen vorm van "hinderlijk volgen", beter bekend als "stalken" kunnen opleveren, immers de wetgever heeft in artikel 426bis WvSr vastgelegd dat er sprake moet zijn van hinderlijk volgen of opdringen op de fysieke openbare weg, niet op de digitale snelweg.

heeft Hyves inmiddels in haar Algemene Voorwaarden een regeling getroffen over overlijden van gebruikers. Pas als er een kopie van een overlijdensakte (zie artikel 1:19g BW) is verzonden naar en ontvangen door Hyves, zal een pagina uit de lucht worden gehaald wegens overlijden. Voor de familie of bekenden een vervelende formaliteit, maar begrijpelijk in het licht van het beschreven misbruik.

8.4 Bewustwording impact persoonlijke informatie

De "International Working Group on Data Protection in Telecommunications" – de "Berlijn Werkgroep" - heeft tijdens een vergadering op 3 en 4 maart 2008 voor alle partijen die bij sociale netwerksites betrokken zijn, een reeks aanbevelingen aangenomen om de persoonsgegevens van netwerkdeelnemers te beschermen en te beveiligen. Service providers wordt in ieder geval aangeraden privacy-vriendelijke 'default settings' te gebruiken. Enkele aanbevelingen zijn verder: geef gebruikers het recht om onder pseudoniem te werken en wees duidelijk naar de gebruikers over de benodigde gegevens. Ook wordt geadviseerd de gebruikers goed voor te lichten over de risico's van het geven van persoonlijke informatie.

Op sociale netwerksites en bij andere Web 2.0 toepassingen geven mensen informatie over zichzelf en kunnen daarbij zelf bepalen hoe ver ze daarin gaan. Een privacy policy voor een dergelijke site kent dus inherente beperkingen. Wel is van belang om – zoals ook aangegeven door de Berlijn Werkgroep - gebruikers goed te informeren over de eventuele risico's die ze lopen als ze online zijn. Vooral moeten de gebruikers bewust worden van de mate waarin ze persoonlijke informatie over zichzelf prijsgeven.

Gebruikers zijn zich namelijk vaak niet bewust van hoe zeer hun informatie echt 'op straat ligt' als ze bijvoorbeeld hun juiste persoonsgegevens op een site als Hyves zetten. Al zijn het dan je 'vrienden' (althans... die term gebruikt Hyves), ken je die mensen ook 'echt'? Weet je zeker dat er niet toevallig iemand tussen zit die misbruik van je wil maken als je bijvoorbeeld vertelt wanneer je op vakantie gaat?

Personen die informatie plaatsen moeten zich bewust zijn van het feit dat niet iedereen graag met allerlei verhalen en beeldverslagen op internet te vinden wil zijn. Het is echter de vraag of bewustwording voldoende is om deze door niet iedereen gewenste transparantie te stoppen. En voorzover het mogelijk is, zal het zeker niet door iedereen als wenselijk worden gezien. Als je graag mensen laat delen in wat je meemaakt, ligt het niet voor de hand bij iedere vermelding van anderen toestemming hiervoor te vragen. Wat wel denkbaar is dat mensen waar mogelijk zoveel mogelijk informatie plaatsen die niet tot specifieke personen herleidbaar is, zeker als hierom gevraagd wordt. Deze verlangde anonimisering is echter niet eenvoudig afdwingbaar. De vrijheid van een ieder zijn mening te uiten is een belangrijk goed en zal afgewogen moeten worden tegen het belang van degene die niet van die uiting gediend is.

8.5 Informatie bij sollicitaties

Bij sollicitaties werd met name in het verleden om referenties gevraagd. Informatie bij deze personen inwinnen heeft in de regel beperkt nut, omdat een sollicitant referenties zal aanvoeren die een positief beeld schetsen. De toekomstige werkgever kan bij een sollicitatieprocedure ook zelf personen benaderen die iets over de beoogde kandidaat kunnen vertellen. In die gevallen wordt de kandidaat gevraagd of het goed is dat er informatie wordt ingewonnen. Indien het een hem/haar minder gunstig gezinde referent is, biedt deze gevraagde voorafgaande toestemming de mogelijkheid om bij de toekomstige werkgever al voorafgaand aan de in te winnen informatie kanttekeningen te plaatsen.[195] Dit beleid raakt door de opkomst van het internet en met name Web 2.0 vertroebeld.

8.5.1 Natrekken sollicitant

Vormt het natrekken van sollicitanten een inbreuk op privacy?[196] Informatie wordt veelvuldig door personen zélf openbaar gemaakt door het op hun eigen site te plaatsen. Het in het Amerikaanse recht bekende criterium 'reasonable expectation of privacy' is via

[195] Dit is uiteraard een duivels dilemma. Door niets te zeggen loop je het gevaar dat negatieve informatie door de referent wordt geuit. Door geen toestemming te geven, wordt duidelijk dat de referent geen positieve informatie zal geven.
[196] Zie hierover D. Demuynck, Sociale netwerksites en arbeidsrecht: nieuwe technologie, nieuwe uitdagingen, *Computerrecht* 2010/3.

het Europese Hof voor de Rechten van de Mens het Nederlandse recht nadrukkelijk binnengedrongen:

> "wat mag men in de gegeven omstandigheden, gelet op de heersende maatschappelijke opvattingen verwachten aan privacy, en welke verwachtingen horen daarbij gehonoreerd te worden?".[197]

Volgens Engelfriet[198] zal de *aard* van de sociale netwerksite de doorslag moeten geven. Doel van deze sites is immers het delen van (persoonlijke) gegevens met familie en "vrienden". Het is verdedigbaar dat er door het naspeuren van een sollicitant geen inbreuk op zijn privacy wordt gemaakt. Wie informatie over zichzelf op internet zet, loopt het risico hier op een later tijdstip mee geconfronteerd te worden en zal hier zelf de gevolgen voor moeten dragen.

8.5.2 Door anderen geplaatste informatie

In het geval de sollicitant de betreffende informatie (schokkende foto's en/of filmpjes) niet op internet heeft gezet, gaat het hierboven gegeven argument niet op. In dat geval is het immers niet persoonlijke informatie die door de sollicitant ter beschikking is gesteld. Het is voor werkgevers echter niet altijd na te gaan wáár de betreffende informatie vandaan komt en bovendien zal een eventueel oordeel door een toekomstige werkgever snel geveld zijn. Van den Hoven van Genderen en Lodder[199] stellen in dit kader het navolgende voor:

> "Eigenlijk zou het aan (toekomstige) werkgevers niet mogen worden toegestaan gebruik te maken van andere, dan door de betrokkene beschikbaar gestelde informatie".

Behalve dat het "checken" van sollicitanten zoals reeds betoogd een geïntegreerd onderdeel vormt van sollicitatieprocedures, is dit voorstel niet gemakkelijk uit te voeren.

In theorie is het voor de betrokken sollicitant mogelijk een actie gebaseerd op artikel 6:162 BW in te stellen tegen een werkgever die op basis van op internet gevonden informatie zonder weder-

[197] EHRM 3 april 2007, *NJ* 2007, 617 met noot EJD.
[198] Zie zijn bijdrage "Bescherming persoonsgegevens 2.0", *Tijdschrift voor Internetrecht*, Nr. 2. mei 2008.
[199] In hun artikel "Informatie leveren tegen elke prijs? Verkenning van het recht rond Web 2.0", *Tijdschrift voor Internetrecht* nr.1, maart 2008.

hoor besluit iemand niet in dienst te nemen. Deze oplossing is in de praktijk niet eenvoudig te realiseren.

Allereerst is er een bewijsprobleem. Indien een werkgever schokkende informatie over een sollicitant aantreft en hierop besluit de kandidaat niet aan te nemen, is het aan de sollicitant om aan te tonen dat hij op deze grond is afgewezen. Het behoeft geen nadere uitleg dat dit de sollicitant in een zeer lastig parket brengt. Ter illustratie kan de volgende opmerking van de Commissie Gelijke Behandeling dienen:[200]

> "krijgen klagers over discriminatie bij de sollicitatie minder dan gemiddeld gelijk"

Het blijkt in de praktijk bijzonder moeilijk aan de bewijsvraag te voldoen. Indien het de sollicitant tóch lukt om te bewijzen dat hij op grond hiervan niet is aangenomen, dient aan te tonen wat precies de schade is die hij/zij geleden heeft. Het eigenlijke doel, aangenomen worden, is niet realiseerbaar.

8.5.3 NVP sollicitatiecode

De Sollicitatiecode van de Nederlandse Vereniging voor Personeelsmanagement en organisatieontwikkeling (NVP) van oktober 2009 bepaalt:[201]

> Indien de arbeidsorganisatie inlichtingen over de sollicitant wil inwinnen bij derden en/of andere bronnen, vraagt zij hiertoe vooraf diens toestemming, tenzij zulks niet vereist is op grond van een wettelijk of algemeen verbindend voorschrift. De te verkrijgen informatie moet direct verband houden met de te vervullen vacature en mag geen onevenredige inbreuk maken op de persoonlijke levenssfeer van de sollicitant. De bij derden en andere bronnen, waaronder websites, verkregen informatie zal, indien relevant, a) aan de sollicitant worden meegedeeld, met uitdrukkelijke vermelding van de bron en b) met de sollicitant worden besproken.

Op grond van deze code moet je dus toestemming vragen voordat je iemand mag googelen of opzoeken op Hyves. Men zou dit kun-

[200] In het jaarverslag van 2007, p. 58.
[201] www.nvp-plaza.nl

nen afvangen met een duidelijke waarschuwing bij de advertentie ("Een achtergrondcheck met Google alsmede een psychologisch onderzoek maken deel uit van de procedure").

8.6 Persoonlijke informatie van jongeren

De discussie over profielen op sociale netwerksites van jongeren onder de 16 wordt al langer gevoerd. Sommigen juristen stellen dat deze profielen in feite illegaal zijn. De basis hiervoor is artikel 5 van de Wet Bescherming Persoonsgegevens (Wbp). Dit artikel bepaalt dat de voor verwerking noodzakelijke toestemming door de ouders gegeven moet worden als de persoon in kwestie nog geen zestien jaar is. Hyves en andere profielsites schenden de privacywet omdat ze de ouders niet om toestemming vragen om profielen van minderjarige deelnemers aan te maken en te publiceren.

Leeftijdsgrenzen voor gebruikers varieert van 13 bij Facebook, Myweb en Twitter tot 16 bij Hyves, of ook jonger met toestemming van de ouders of wettelijk vertegenwoordiger. Dit lijkt een wat vroege leeftijd om deel te nemen aan door volwassenen bevolkte sociale netwerksites en overigens niet in lijn met de door dezelfde aanbieders ondertekende gedragsregels ter bescherming van kinderen en jeugdigen.[202]

In Nederland is het alleen toegestaan om persoonsgegevens te verwerken of gebruiken als er toestemming is van de persoon om wiens persoonsgegevens het gaat. De Wbp is hierin strenger dan de situatie waarin kinderen bijvoorbeeld iets kopen in een winkel. Hiervoor is formeel genomen toestemming van de ouders nodig, maar die wordt geacht te zijn gegeven als de aankoop "normaal" is voor een kind van een bepaalde leeftijd. Op het internet moeten ouders iedere keer expliciet toestemming geven voor de verwerking van de persoonsgegevens van hun kinderen, en mag de site niet vooraf aannemen dat deze gegeven is.

Ouders blijven hoe dan ook verantwoordelijk voor de rechtshandelingen van hun kinderen. Ter vergelijking, buiten contract (feitelijk

[202] Safer Social Networking Principles voor de EU. http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

handelen) zijn ouders aansprakelijk bij kinderen onder de 13 jaar (artikel 6:169 lid 1 BW) en voor kinderen van 13 en 14 jaar (artikel 6:169 lid 2 BW) indien de ouders een verwijt kan worden gemaakt.

8.7 Spam via krabbels?

Vanzelfsprekend zijn de doelgroepen en de profielen van de sociale netwerken interessant voor marketing doeleinden. Niet alleen de deelnemers zelf maar ook bedrijven willen graag laten zien wat zij te bieden hebben.

Daarbij is het niet altijd even duidelijk of het bedrijf rechtmatige bedoelingen heeft. Zo werd een "spammer" beboet door OPTA voor het verzenden van spam op het Hyves netwerk.[203] Onderzoek van OPTA had uitgewezen dat een privé persoon meer dan 3 miljoen ongevraagde krabbels verstuurde vanuit automatisch aangemaakte Hyves-profielen. Het is de eerste keer dat OPTA een boete uitdeelt voor het versturen van spam via een sociale netwerksite. Raymond Spanjar, medeoprichter van Hyves, was verheugd dat OPTA haar activiteiten met betrekking tot het bestrijden van spam uitgebreid heeft tot activiteiten op sociale netwerksites:

> "Social networks zijn potentieel spam-vrije communicatieplatformen omdat er vooral door vrienden onderling wordt gecommuniceerd. Die vertrouwde omgeving wordt bedreigd door spammers. We zijn dan ook erg blij dat dankzij deze uitspraak van OPTA spam voortaan hard aangepakt kan worden"[204]

Een voorbeeld van agressieve marketing via netwerksites zoals Hyves is een uitnodiging die jongeren kregen van Fotosessie.com voor een fotoshoot. Hierbij wekte Fotosessie.com de indruk dat de 'kandidaat' speciaal was gekozen vanwege zijn uiterlijk. De fotoshoot zou een opstap zijn voor een carrière als model. Ook leek het te gaan om een speciale aanbieding die niet lang geldig zou zijn. Uit onderzoek is gebleken dat dit allemaal niet waar was. Daarom is er sprake van misleidende en agressieve verkoop. Consumenten die niet naar de afspraak kwamen kregen per post

[203] Zie ook A. Engelfriet (2010), Ongevraagd commercieel krabbelen: 12.000 euro boete, *Tijdschrift voor internetrecht* 2010/1.
[204] Te vinden op www.spamklacht.nl

aanmaningen, invorderingen en prijsverhogingen voor een niet geleverde prestatie.

9 Verwijderen persoonlijke informatie van internet

De digitale sporen van eenmaal op internet geplaatste teksten, foto's, filmpjes, etc. zijn niet eenvoudig te wissen. Het geheugen van internet is in potentie eindeloos. Voor positieve informatie is dit in beginsel geen probleem, maar voor negatieve informatie veelal des te meer. Dat is vervelend als je zelf deze informatie op internet plaatst, maar voor informatie die buiten jou om op het internet is gezet is dit des te vervelender. Te meer daar je er lang niet altijd weet van hebt dat deze informatie bestaat.

Als je er achter komt dat er ongewenste informatie van jou op internet te vinden is en je wilt dit laten verwijderen dan geldt het adagium "bezint eer ge begint". Het is bekend dat ruchtbaarheid vaak averechts werkt. Een door vrijwel niemand opgemerkt filmpje of foto krijgt veel meer aandacht als er een zaak van gemaakt wordt. Rechtstreekse communicatie werkt hier vaak het beste, zoals begin 2008 bij een verzoek van iemand die in een oude voor hem vervelende rechtszaak met naam en toenaam genoemd werd. Bij het intikken in Google van zijn naam verscheen deze zaak als eerste treffer. Doordat deze persoon de redactie van de jurisprudentiebundel benaderde, was de informatie binnen een week volledig uit Google verdwenen.

In dit hoofdstuk word de informatie over personen op Web 2.0 toepassingen behandeld aan de hand van Nederlandse rechtspraak over Hyves.[205] Het hoofdstuk is opgesplitst in een deel over opzettelijk negatieve uitingen en andere negatieve gevolgen die de informatie op profielen kan hebben.

9.1 Opzettelijk negatieve uitingen op een profiel

Het overgrote deel van rechtszaken over sociale netwerksites gaat over negatieve uitingen. Achtereenvolgens wordt ingegaan op

[205] De volgende paragrafen zijn ontleend aan A.R. Lodder, Schadelijke of ongewenste informatie op sociale netwerksites, *Computerrecht* 2010/3.

ontevreden kopers, een slecht functionerend dierenpension en over een controversiële advocaat.

9.1.1 Ontevreden kopers

Ontevreden kopers hebben in internet een medium gevonden waar ze eenvoudig hun teleurstelling over niet naar tevredenheid verlopen transacties kunnen ventileren. De traditioneel zwakkere partij, reden waarom er consumentenrecht bestaat, heeft met dit openbare klaagrecht een sterk middel in handen.

Veel ophef en een reeks vonnissen is er geweest rond de van oplichting beschuldigde verkopers van Trendylaarzen.[206] Voordat negatieve berichten geplaatst werden op de in deze uitspraken centraal staande site internetoplichting.nl waren er negatieve berichten op Hyves verschenen.[207] Hyves werkte mee aan een verzoek om deze uitingen te verwijderen en verschafte ook de NAW gegevens van enkele anonieme klagers. Een van de anonieme klagers bleek een concurrent. Opmerkelijk is wel het gemak waarmee deze uitingen verwijderd werden en de NAW gegevens doorgespeeld. Uiteindelijk bleek Trendylaarzen daadwerkelijk schuldig aan oplichting[208] en heeft Hyves dus ten onrechte de berichten weggehaald. Saillant is dat de oplichting eruit bestond dat consumentrechten werden geschonden. De zwakkere partij werd dus ten onrechte haar wettelijke rechten onthouden, maar sloeg hard terug via het plaatsen van uiteindelijk geoorloofde negatieve berichten. Als één van de oplichtingspraktijken werd vooruitbetaling van de gehele prijs genoemd. Dit is weliswaar wettelijk verboden (artikel 7:26 lid 2 BW), maar in de praktijk van internethandel dermate gebruikelijk dat dit niet echt als oplichting kan worden gezien. Wel een duidelijk geval van oplichting is het vervolgens niet leveren en ook niet terugbetalen van het vooruitbetaalde geld.

[206] De in april 2009 gehouden FLITS IX bijeenkomst *De spagaat van providers en forumbeheerders: wanneer zijn ze (niet) aansprakelijk voor geplaatste content?* was hieraan gewijd, zie http://lodder.cli.vu/flits.
[207] Vzr. Amsterdam 12 maart 2009 (LJN BH7529). Opmerkelijk is dat in deze zaak gesproken wordt over berichten op Hyves sinds augustus 2008 en in de latere zaak Vzr. Amsterdam 2 juli 2009 (LJN BJ1669) het gaat om berichten sinds november 2008. In deze laatste zaak wordt ook aangegeven dat de site Trendylaarzen actief was vanaf september 2008 wat klachten een maand daaraan voorafgaand onmogelijk maakt.
[208] Vzr. Amsterdam 2 juli 2009 (LJN BJ1669).

Een jaar eerder diende er bij de Rechtbank Zwolle[209] een zaak over een ontevreden bruid. Hier ging het niet om het schoeisel, maar om de aangeschafte jurk. Op verschillende plaatsen laat deze bruid negatieve berichten achter. Zo waarschuwt ze op Hyves anderen om niet naar de bruidsmodezaak te gaan:

> "dat veel bruidjes zijn opgelicht en dat al veel meiden de dupe zijn geworden."

De vraag die in deze zaak centraal staat is niet of je al dan niet mag klagen wanneer je ontevreden bent over de dienstverlening, maar

> "wanneer de desbetreffende uitlatingen de grens van de in het maatschappelijke verkeer betamelijke zorgvuldigheid overschrijden en mitsdien als onrechtmatig gekwalificeerd moeten worden."

Daar is in deze zaak sprake van. Hierbij speelt minder de aard van de uitingen, maar gaat het vooral om de feitelijke onjuistheid.

De in de uitspraak opgelegde rectificatie is niet in tijd beperkt. In de eis was ook enkel aangegeven "te plaatsen en geplaatst te houden" zonder een einddatum, dus in beginsel oneindig. Mogelijk is dit ingegeven door het feit dat ook de negatieve berichten nog jarenlang op internet kunnen rondzwerven, maar het bevreemdt wel dat iemand veroordeeld wordt tot het plaatsen van een rectificatie voor onbepaalde tijd. In de uitspraak is daarnaast niet aangegeven hoe de rectificatie dient te zijn opgemaakt.[210] Dit laatste is minder een probleem, aangezien de rectificatie op de site van de verkoopster moet worden geplaatst, te weten www.trouwshop.com:

> "RECTIFICATIE M.B.T. [eiseres]
> Ten onrechte heb ik in de periode [periode] tot en met heden op diverse internetfora over [eiseres] te [woonplaats] en [eiseres] in persoon opmerkingen geplaatst zoals "ik ben echt in staat om haar helemaal kapot maken", "ik heb liever dat ze failliet gaat", "iedereen moet voor haar gewaarschuwd worden", "ze moet aangepakt worden", "gaan jullie me helpen haar op te houden met deze praktijken" en de

[209] Rechtbank Zwolle 9 mei 2008 (LJN BD 1358)
[210] Zie over deze problematiek A.R. Lodder. Wat is een homepage? - Noot bij Vzr. Amsterdam 7 december 2005. *Mediaforum* (3), 2006.

> uitlating dat "ze een viese oplichter is". Ik neem voormelde door mij gedane beschuldigingen en uitlatingen terug. Ten onrechte heb ik derden opgeroepen niet naar [eiseres] te [woonplaats] te gaan.
> De voorzieningenrechter van de rechtbank Zwolle-Lelystad heeft geoordeeld dat die voormelde door mij gedane uitlatingen, beschuldigingen en oproep onrechtmatig zijn jegens [eiseres] en [eiseres] in persoon.
> [gedaagde] [gedaagde]/[gebruikersnaam].",

Of het puriteins of wellicht zelfs gebruikelijk is (dat de te rectificeren tekst identiek moet zijn aan de oorspronkelijke) of een verschrijving, in de rectificatie moet in ieder geval volgens het vonnis komen te staan "viese oplichter".

9.1.2 Mishandeling in het dierenpension

In 2007 werd een dierenpensionhoudster beschuldigd van onder andere zware verwaarlozing van dieren. Onnodig grievende teksten van de orde

> "En met d'r kinnebak over het asfalt trekken"

en

> "(…) ik heb haar in mijn droom toch heerlijk toegetakeld zeg helemaal geweldig. en ze was zoooo bang"

staan na de daarop volgende veroordeling wegens smaad[211] in de zomer van 2007 niet meer op internet. De inzet van het kort geding in januari 2008[212] was deels om de gegevens van personen die achter een "hate-pagina" op Hyves zitten en degenen die op Hyves negatieve berichten plaatsen te achterhalen. Voor wat betreft de negatieve uitingen is de eis verstrekkend:

> "Hyves te gelasten (…) alle teksten over en met betrekking tot de persoon en het bedrijf van eiseres verwijderen van hun websites dan wel de toegang daartoe volledig en blijvend onmogelijk maken."

De informatie die in dit kort-geding met name aan de orde is, is een oproep tot een demonstratie op 12 januari 2008 tegen de

[211] Politierechter te Zwolle-Lelystad 24 augustus 2007 (LJN onbekend).
[212] Vzr. Arnhem 10 januari 2008 (LJN BC2736).

pensionhoudster. Op Hyves was een foto van een verbrande hond geplaatst en in de oproep onder andere de volgende teksten:

> "Deze mishandelingen moeten gestopt worden (…)"

en

> "Dierenhotel Tolhuis wordt geleid door iemand die voor de AID werkt en der eigen vleeswaren keurt in opdracht van de Overheid en verwaarlozing niet schuwt."

De rechter is van oordeel dat er geen reden is de oproep tot deze demonstratie te verbieden en dat Hyves dus ook niet verplicht kan worden deze oproep ("laat staan alle berichten met betrekking tot de persoon en het bedrijf van eiseres") te verwijderen. Gegevens over gebruikers van Hyves hoeven derhalve ook niet te worden verstrekt. Mogelijk dat Hyves haar beleid om informatie weg te halen en NAW-gegevens te verstrekken later heeft versoepeld, want zoals hierboven bleek waren ze in 2009 bij Trendylaarzen – ten onrechte – daartoe bereid.

9.1.3 De vermeend pedofiele, schietende advocaat

Op 4 maart 2010 wees het Hof Amsterdam[213] een arrest over beweerdelijk onrechmatige uitingen op een Hyves profiel. In een weblog op een Hyves-profiel is van alles beweerd over een advocaat, maar de kern van deze zaak komt op het volgende neer:

> "Het grootste geschil tussen partijen spitst zich toe op de vraag of [principaal geïntimeerde] onrechtmatig jegens [principaal appellant] heeft gehandeld door zich in een weblog op haar hyves-pagina negatief uit te laten over [principaal appellant]."

De vrijheid van meningsuiting is een belangrijk goed en kan - zoals in de internetoplichting zaak - een beschuldiging aan het adres van een ander inhouden. Zoals bij ieder grondrecht is ook hier inperking mogelijk. Het Hof geeft als begrenzing

> "in het geval daarmee iemands eer en goede naam op onrechtmatige wijze wordt aangetast."

[213] Hof Amsterdam 4 maart 2010 (LJN BL 6050)

Het aantasten van de eer en goede naam is op zichzelf geen voldoende reden. Anders zouden er nooit beschuldigende uitingen zijn toegestaan. De aantasting moet echter niet zo ver gaan dat deze als onrechtmatig kan worden gezien.

Van belang in deze zaak is dat het anders dan bijvoorbeeld bij de bruidsmode om een besloten Hyves-profiel ging. Wel was het mogelijk dat naast de "echte" vrienden ook 'vrienden van vrienden' toegang tot het profiel kregen. Echter, deze indirecte vrienden kregen pas toegang nadat ze nadrukkelijk toegelaten werden. Binnen deze relatief kleine kring werden de volgende uitingen *niet* onrechtmatig geacht:

> "- de kwalificatie van hem als 'kermisattractie';
> - de uitlating dat hij een klein manneke van 1.60 m is;
> - de suggestie dat hij het moet hebben van 'vriendjes van het ministerie';
> - de suggestie dat hij de domeinnaamhouder van [website], waarop een artikel werd gepubliceerd over wat er in de rechtszaal gebeurde, heeft bedreigd;
> - de suggestie dat hij zich voorgedaan zou hebben als '[naam]' en [principaal geïntimeerde]s hyves heeft gekopieerd;
> - de suggestie dat hij een jachtgeweer nodig heeft om bij [principaal geïntimeerde] op de koffie te komen;
> - de uitlating "You fucked with the wrong women!";
> - de suggestie dat hij gebruik zou maken van een Amerikaans IP-adres ("Wat een scheiterd of niet?")."

De aard van de uitingen en de te verwachten gevolgen worden niet ernstig genoeg geacht. Wat betreft het jachtgeweer kan worden verwezen naar het door deze advocaat gebruikte visitekaartje waarop hij stond afgebeeld met pistool en jachtgeweer en het motto "eerst schieten, dan praten."[214]

Wel onrechtmatig werd beoordeeld de uiting dat de advocaat een veroordeelde pedofiel was. Hierover bestond overigens tussen partijen geen onenigheid. De enige toevoeging in deze zaak ten opzichte van de eerste aanleg is dat het verbod om dergelijke uitingen in de toekomst te doen via publicaties op internet is uitgebreid met 'chatgesprekken'. Dit is opmerkelijk, want in beslo-

[214] Hiervoor is de advocaat tuchtrechtelijk veroordeeld, althans hij heeft in 2009 een waarschuwing gekregen van het Hof van Discipline, zie http://www.advocatie.nl/page?1,3221/Personen/rambo_kuijpers_part_ii

tenheid mag doorgaans gezegd worden wat men wil. Een merkwaardige consequentie is dat in een chat-gesprek niet, maar in een gewoon telefoongesprek (of skype-gesprek) ook na dit vonnis nog gezegd mag worden dat de advocaat een veroordeelde pedofiel is.[215] Vermeldenswaard is tenslotte de niet toegewezen rectificatie die geëist werd, omdat deze in tegenstelling tot de wel toegewezen rectificatie bij de bruidsmodezaak bijzonder precies omschreven is (en beperkt in tijd):

> "[principaal geïntimeerde] zal veroordelen tot het onafgebroken 24 uur per dag op elke kalenderdag gedurende zes maanden na betekening van het te wijzen arrest op de eerstzichtbare pagina van een door [principaal geïntimeerde] te (her)openen profiel op www.hyves.nl, zonder pop-ups en zonder enig commentaar op internet of in de gedrukte media, omgeven door een zwart kader, in zwarte letters, met lettertype Arial in puntsgrootte 12, op een witte achtergrond, de volgende tekst te ondertekenen en te plaatsen en [principaal appellant] daarvan op elke kalenderdag gedurende genoemde periode per e-mail [emailadres] of per fax [faxnummer] het bewijs van plaatsing (digitale screenshots of papieren kopieën) van onderstaande tekst te leveren:"

Met name de eis om iedere dag een bewijs van plaatsing te leveren leent zich niet voor toewijzing. Als een rectificatie op Hyves staat en iemand wil weten of dit iedere dag zo is, kan hij dit eenvoudig zelf vaststellen.

9.2 Andere negatieve gevolgen profiel

In de tot nu toe besproken gevallen is steeds de plaatser van informatie zich bewust van de mogelijk negatieve gevolgen hiervan. Informatie kan gebruikt worden op een niet gewenste manier en lang niet altijd is het mogelijk hier adequaat tegen op te treden. Achtereenvolgens zal worden ingegaan op de vraag of iemand die een Hyves-profiel heeft zich niet meer kan verzetten tegen inbreuken op zijn persoonlijke levenssfeer, het leggen van contact via Hyves en door het subject zelf geplaatste informatie.

[215] Een mogelijke verklaring zou kunnen zijn dat Hyves chat met een groep vrienden mogelijk maakt. Hoewel dit de achterliggende gedachte bij de uitspraak kan zijn geweest, blijft de keuze voor chat dan betrekkelijk willekeurig. Diezelfde groep vrienden kan immers op verschillende andere wijzen communiceren zoals in een virtuele wereld of als fysieke groep.

9.2.1 Inbreuken op persoonlijke levenssfeer van de eigenaar van een profiel

Zoals al eerder naar voren is gekomen, is de beslissing van gedupeerden om een rechtszaak te beginnen lastig. De Maastrichtse praeses die graag van Dumpert verwijderd wilde worden met de beelden die van haar in dronkenschap waren opgenomen, kreeg door haar rechtszaak veel aandacht.[216] Het in deze zaak door Geenstijl naar voren gebrachte argument dat je geen beroep kan doen op bescherming van de persoonlijke levenssfeer als je een Hyves-profiel hebt is terecht door de rechter aan de kant geschoven:

> "Geenstijl heeft nog aangevoerd dat [eiseres] het aan haar zelf te wijten heeft dat Geenstijl het filmpje openbaar gemaakt heeft (…) ook omdat haar recht op privacybescherming beperkt zou zijn, onder meer omdat zij een voor iedereen toegankelijke 'hyves' pagina zou hebben."

Het is op zichzelf juist dat door het openen van een Hyves-profiel je een deel van je privé-leven prijs geeft. Het betekent uiteraard niet dat dit anderen in algemene zin legitimeert om zonder toestemming tot de persoon herleidbare informatie op internet te plaatsen.

Wel kan gesteld worden dat als iemand bijzonder actief is op zijn profiel en daar veel informatie plaatst, de kans op inbreuk op de persoonlijke levenssfeer afneemt. De bekende mantra "ik heb niets te verbergen"[217] lijkt vooralsnog overigens niet breed gedragen als het om op internet geplaatste informatie gaat, maar zich te beperken tot maatregelen op het terrein van terrorismebestrijding.

9.2.2 Niet gewenst contact

Het aanknopen van contacten via Hyves wordt geschaard onder contactverboden zoals in het geval van ex-echtelieden.[218] Soms

[216] Vzr. Amsterdam 11 september 2009 (LJN BK1859). Zie ook http://jurel.nl/2009/10/28/dronken-maastrichtse-praeses-culpa-in-causa/
[217] Solove, D.J. (2007), 'I've Got Nothing to Hide and Other Misunderstandings of Privacy', San Diego Law Review 44 (2007): 745 en http://jurel.nl/2007/06/18/ik-heb-niets-te-verbergen-maar-hecht-wel-aan-mijn-persoonlijke-levenssfeer/
[218] Rb. Haarlem 19 mei 2009 (LJN BJ1038).

wordt dit verbod ook duidelijk geschonden, zoals de vrouw die op Hyves het bericht plaatste:

> "Hey dikke eh dikkie sorry, laat [naam 2] [de man, hof] dit berichtje even lezen a.u.b. wat nou als ik al je homofoto's en films op mijn hyves zet!!! blijf je het dan nog ontkennen??? wordt moeilijk denk ik. Mijn hyves wordt nogal veel bekeken."[219]

Enigszins in strijd met de slotzin voerde de vrouw als verweer dat dit bericht niet voor iedereen toegankelijk is, maar alleen voor vrienden en kennissen. Dit besloten profiel had niettemin bijna honderd vrienden, waarmee het bericht ruime bekendheid heeft verkregen en duidelijk een schending van het contactverbod oplevert.

Interessant is een vader die bij de benoeming van een curator meent dat de moeder niet op de hoogte hoeft te worden gehouden van de ontwikkeling van haar dochter, omdat ze dat via Hyves al doet. Hier gaat de rechter, begrijpelijk, niet in mee.[220]

9.2.3 Door het subject zelf geplaatste informatie

Iedereen moet zich realiseren dat informatie op Hyves, zeker bij een openbaar profiel, door anderen gebruikt kan worden.[221] Dit gebruik kan onschuldig zijn, zoals in de zaak van een vermeende meesteroplichter:[222]

> "Van mensen die hem kennen hoorde ik dat hij zo leuk is met zijn kinderen. Ik geloof het direct. Hij heeft ook nog een vrouw zag ik op Hyves, lijkt me op eerste gezicht ook best aardig. Maar die moet toch wel een beetje een vermoeden hebben dat haar man gewetenloos andere mensen in het verderf stort, alleen om geld."

Dat je door foto's iemand zijn vrouw kan identificeren is op zichzelf niet ernstig, hoewel er onder omstandigheden misbruik van gemaakt kan worden. Zo werden de kinderen van een bij de politie werkende vrouw werden bedreigd omdat via foto's van iemand Hyves-account duidelijk werd waar haar kinderen op school zaten.

[219] Hof Leeuwarden 19 november 2008 (LJN BG4804).
[220] Hof Amsterdam 9 februari 2010 (LJN BL5778).
[221] Zie ook paragraaf 8.5.
[222] Rb. Almelo 7 april 2008 (LJN BC8930).

Soms zijn de verwijzingen naar foto's op Hyves onaangenaam. In een e-mail of SMS-bericht werd gezegd:

> "zeg effe tegen die kankerkop uit Velden dat als hij op Hyves zit dat hij de foto effe wat groter maakt, zodat ik de goeie voor heb me heb !! voordat ik de verkeerde opruim"[223]

Hyves kan gebruikt worden ter identificatie, niet alleen van beoogde slachtoffers zoals in dit geval, maar ook voor het traceren van daders. Ook opsporingsinstanties hebben de bruikbaarheid en bereikbaarheid van profielen op sociale netwerksites ontdekt.[224]

Je kunt ook jezelf in verlegenheid brengen. De voetballer Van der Wiel reisde najaar 2009 niet af met de nationale ploeg vanwege een hersenschudding. Op zijn Twitter-account plaatste hij vervolgens tweets over zijn concertbezoek van rapper Lil' Wayne in de Heineken Music Hall.[225] Hoewel het tegen een bal koppen schadelijker is voor iemand met een hersenschudding dan een rapconcert bijwonen, was niet verstandig dit uitstapje breed uit te meten via Twitter. In reactie op de ophef die naar aanleiding van deze tweet is ontstaan, zijn onder andere voetballers van Ajax gestopt met twitteren. In dit geval kon de plaatser van de informatie bedenken dat het delen van deze informatie consequenties kon hebben. Er zijn ook situaties waar de plaatser van informatie niet voldoende bedacht is op gebruik of misbruik door derden van de gedeelde informatie. Door gebruikers bewust te maken van de risico's, kunnen ze een betere inschatting maken over welke informatie ze beter wel en niet kunnen delen.

9.3 Slotopmerkingen

Er zijn gevallen waarbij de juridische grondslag om actie te ondernemen minder sterk is. Het zal dan vrijwel altijd neerkomen op een niet gewenste schending van de persoonlijke levenssfeer. Inbreuken op de persoonlijke levenssfeer (Wbp, portretrecht Aw) zijn geen absolute rechten maar zullen afgewogen moeten worden

[223] Rechtbank Roermond 26 september 2008 (LJN BF22270). In deze zaak volgde een veroordeling voor belaging (artikel 285b Sr). Vgl. Rb. Breda 30 oktober 2009 (LJN BK1696) waarin ook veroordeeld werd voor belaging via onder meer Hyves.
[224] Zie paragraaf 2.3.2
[225] http://www.depers.nl/sport/344256/Van-der-Wiel-schrikt-van-ophef.html

tegen het belang dat de plaatser van de informatie erbij meent te hebben.

Personen die graag in de anonimiteit blijven, zullen in de toekomst steeds vaker via sociale netwerksites van vrienden traceerbaar zijn. Handmatig of met behulp van data mining software kan zo betrekkelijk eenvoudig via berichten, foto's, krabbels, Tweets, etc. een redelijk compleet beeld verkregen worden van een willekeurig persoon. Zelf anoniem blijven of niet op de netwerksites actief zijn, helpt daarbij maar ten dele. Er hoeft immers maar één stapvriend een foto te plaatsen met "ik en Arno lekker zat!" erbij en de heer Lodder heeft op zijn werk en/of thuis mogelijk iets uit te leggen.

Op Hyves-profielen is bijzonder veel informatie te vinden. Negatieve berichten worden soms door Hyves weggehaald en NAW-gegevens doorgespeeld (Trendylaarzen 2009), maar in andere gevallen werkt Hyves niet mee (Dierenpension 2008). De rechter staat veel uitingen toe, maar 'pedofiel' wordt zowel strafrechtelijk als civielrechtelijk als ontoelaatbaar gezien. Bij andere uitingen kan de feitelijke juistheid een rol spelen en de te verwachten negatieve gevolgen.

Wat voor iedere eigenaar van een profiel geldt is dat deze zich goed bewust moet zijn van de impact en de gevolgen van de geplaatste informatie. Net als bij andere informatie op internet geldt dat eenmaal op internet aanwezige informatie een lange nasleep kan hebben. De aard van een profiel (laagdrempelig, zoveel mogelijk informatie delen) maakt dat in veel gevallen te gemakkelijk informatie geplaatst wordt. Dit geldt in mindere mate voor negatieve uitingen, omdat de plaatser zich dan doorgaans wel bewust is van de mogelijk negatieve gevolgen.

Toch is het te hopen dat er een ethiek op internet ontstaat met betrekking tot het plaatsen van informatie, zeker ook bij sociale netwerksites, waarbij rekening wordt gehouden met anderen, ook als deze geen juridisch afdwingbare rechten hebben.

Publicatiereeks NVvIR - Nederlandse Vereniging voor Informatietechnologie en Recht

27 *Recht & Web 2.0. Bewerkte bloemlezing uit www.internetrecht20.nl*, A.R. Lodder, R. van den Hoven van Genderen, A. Engelfriet, D. Mekic' e.a., Lulu 2010
26 *Who controls the Internet? Wie bepaalt wat op internet?* E.N.M. Visser & M. Weij (red.), Elsevier Juridisch 2009
25 *Recht en locatie. Geo-informatie in een juridische context*, L. van der Wees & S. Nouwt (red.), Elsevier Juridisch 2008
24 *Open Source Software: Een verkenning naar de juridische aspecten van open source software*, E. Thole, R. Scholten & W. Seinen (red.), Elsevier Juridisch 2006
23 *Recht in een virtuele wereld: Juridische aspecten van Massive Multiplayer Online Role Playing Games* (MMORPG), A.R. Lodder (red.), Elsevier Juridisch 2006
22 *IT Law - The Global Future: Achievements, Plans and Ambitions,* A.R. Lodder, A. Meijboom & D.T.L. Oosterbaan (eds.), Elsevier Juridisch 2006
21 *Privacy en andere juridische aspecten van RFID: Inhoud unieke identificatie op afstand van producten en personen*, G.J. Zwenne & B. Schermer (red.), Elsevier Juridisch 2005
20 *(IT) Outsourcing. Juridische aspecten van outsourcing*, G. Brunt & B. Westerbrink-Veenendaal (red.), Elsevier Juridisch 2004
19 *'Loshetzelfop.nl', ADR in digitale context*, G. Brunt, P. van Schelven & L. van der Wees (red.), Elsevier Juridisch 2004
18 *Privacy concerns. Het delen van persoonsgegevens bij fusies, overnames en binnen concerns,* C. Cuijpers, P. van der Put & J. Terstegge (red.), Elsevier Juridisch 2003
17 *E-communicatie: Visie op een nieuw kader of vissen achter het net?*, R. van den Hoven van Genderen (red.), Elsevier Juridisch 2003

16 *E-marktplaatsen, Juridische aspecten van business to business elektronische marktplaatsen,* S.J.H. Gijrath & H.C. Hoogeveen (red.), Elsevier Juridisch 2002
15 *E-government; virtuele fictie of blijvend toekomstbeeld?*, R. van den Hoven van Genderen (red.), Elsevier Juridisch 2001
14 *De e-consument. Consumentenbescherming in de Nieuwe Economie,* C. Stuurman, R.J.J. Westerdijk, & C. Sander (red.), Elsevier Juridisch 2000
13 *Convergentie in telecom- en mediasector, Recht op informatie in elke vorm*, R van den Hoven van Genderen, A.T. Ottow & C. Stuurman (red.), Samson Bedrijfsinformatie 1997
12 *10 jaar IT & Recht: verleden, heden en toekomst*, Samson Bedrijfsinformatie 1996
11 *Intellectueel eigendom in digitaal perspectief*, S.J.H. Gijrath, R. van den Hoven van Genderen & W. Wefers Bettink (red.), Samson 1996
10 *Recht op de elektronische snelweg? Drie thema's inzake overheidsbeleid en nieuwe mogelijkheden voor informatievoorziening,* J. Nouwt, R. van den Hoven van Genderen & J.E.J. Prins (red.) Samsom Bedrijfsinformatie 1995
9 *Overheidsaanbestedingen in de IT: van onderhandelingsmodel naar aanbestedingsmodel*, S. Corvers, F. van der Klaauw-Koops & W. Wedekind (red.), Samsom Bedrijfsinformatie 1995
8 *Publiekrechtelijke Electronic Data Interchange*, A.H.J. Schmidt & G.J. Zwenne (red.), 1994
7 *Juridische aspecten van artificiële intelligentie*, 1993
6 *Juridische aspecten van het GBA-Project*, E.R. Brouwer, R.J.I. Dielemans, B.R. Dorbeck-Jung e.a., Otto Cramwinckel 1992
5 *Toogdagbundel Juridische Informatiesystemen*, A. Oskamp *et al.* (red.), 1992
4 *Juridische aspekten van netwerken*, F. de Graaf (red.), 1990
3 *Certificatie van software in juridisch perspectief*, 1988
2 Software als zekerheid, E.P.M. Thole, 1988
1 *Preadvies computercriminaliteit. Een reactie op het rapport "Informatietechniek & Strafrecht" van de Commissie Computercriminaliteit, opgesteld ten behoeve van de najaarsvergadering van de NVIR,* R.V. De Mulder e.a., 1987